Titre: Title:	Sur la sécurité des communications aériennes par liaison de données
Auteur: Author:	Corentin Bresteau
Date:	2018
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Bresteau, C. (2018). Sur la sécurité des communications aériennes par liaison de données [Master's thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/3283/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/3283/
Directeurs de recherche: Advisors:	Jose Manuel Fernandez
Programme: Program:	Génie informatique

UNIVERSITÉ DE MONTRÉAL

SUR LA SÉCURITÉ DES COMMUNICATIONS AÉRIENNES PAR LIAISON DE DONNÉES

CORENTIN BRESTEAU
DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
AOÛT 2018

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

SUR LA SÉCURITÉ DES COMMUNICATIONS AÉRIENNES PAR LIAISON DE DONNÉES

présenté par : BRESTEAU Corentin
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

M. BELTRAME Giovanni, Ph. D., président
M. FERNANDEZ José M., Ph. D., membre et directeur de recherche
M. PATTERSON Patrick, membre

DÉDICACE

Une fois que vous aurez goûté au vol, vous marcherez à jamais les yeux tournés vers le ciel, car c'est là que vous êtes allés, et c'est là que toujours vous désirerez ardemment retourner.

. . .

REMERCIEMENTS

Il est important de souligner dans ces travaux l'aide du Pr. José.M. Fernandez, mon directeur de recherche, qui m'a permis de traiter pendant 2 ans un sujet qui me passionne. Les moyens mis à ma disposition étaient en tout temps optimaux ont rendus possible des travaux de recherche exaltants.

Le laboratoire SecSi en général m'a permis de poursuivre mon travail toujours dans une ambiance joviale et appréciée. Je tenais à noter plus particulièrement les apports de Militza Jean pour sa disponibilité constante, sa bonne humeur sans faille et sa patience dans mes nombreuses requêtes, ainsi que l'aide de Paul Berthier qui a travaillé avec moi sur les 2 articles liés à ce mémoire et m'a apporté son expertise sur des problématiques similaires.

Je dois également remercier Gilles Hudicourt, pilote chez Air Transat pour son aide précieuse à plusieurs reprises. Il m'a apporté des informations toujours riches et pertinentes.

Je tiens à saluer ma famille qui m'a laissé vivre une expérience plus que précieuse au Canada grâce à un soutien sans faille sur tous les plans, tout au long de ma vie étudiante et au préalable.

Enfin, je remercie mes amis et amies sur le continent américain et partout autour du globe qui ont rendu chaque jour exceptionnel, et grâce auxquels j'ai pu observer les plus beaux spécimens de rorquals québécois.

RÉSUMÉ

Depuis les jours lointains où les contrôleurs aériens comme Archie League utilisaient des drapeaux pour diriger les appareils en vol, de nombreux progrès technologiques ont permis d'améliorer l'efficacité et la fiabilité des opérations de contrôle. Le transport aérien est dorénavant un mode de locomotion parmi les plus sécuritaires.

Au sein des nouveaux systèmes de communication, on peut relever les liaisons de données, également appelées Datalink, qui permettent aux pilotes, aux contrôleurs ainsi qu'aux compagnies aériennes d'échanger directement des données via les ondes radio. Les nombreux avantages que présentent ces systèmes sur les communications vocales classiques ont rendu leur adoption extrêmement rapide et ils sont maintenant obligatoires sur la plupart des routes aériennes.

Si l'automatisation toujours plus élevée des systèmes aéronautiques permet d'optimiser l'utilisation des espaces aérien, elle présente certains inconvénients. Les performances supplémentaires induites par ces nouveaux systèmes sont malheureusement parfois obtenues aux dépens d'une surface d'attaque accrue. Les composantes avioniques numériques des avions de ligne sont maintenant sensibles à de potentielles cyberattaques, car elles sont intégrées dans un écosystème informatisé complexe. Ce risque est renforcé par la démocratisation récente des radios logicielles (SDR) ainsi que des outils de développement associés. Ces radios logicielles permettent à un nombre accru de potentiels pirates d'intercepter et d'émettre des faux paquets de liaison de données tout en se faisant passer pour des acteurs légitimes. Ceci risque de causer de sérieuses dégradations potentielles des services aériens. Un nombre important de pirates pourrait maintenant se procurer à un prix très faible le matériel nécessaire pour communiquer et interagir avec les systèmes embarqués.

Les protocoles les plus vulnérables aux attaques de spoofing sont les plus anciens comme ACARS et CPDLC. En effet, ils ont été développés entre les années 1980 et 1990, sans aucune considération sur la cybersécurité et ne permettent pas le recourt à des méthodes de protection cryptographiques. Ces protocoles sont néanmoins encore très extensivement utilisés et offrent des cibles de choix pour les potentiels pirates.

Au cours de ces travaux, nous allons présenter l'état actuel des communications par liaisons de données. Nous allons présenter quels sont les systèmes en services et quels sont les outils disponibles pour les sécuriser. Nous allons ensuite mener une analyse de risque sur les protocoles Datalink les plus populaires. Nous allons détailler de quelle manière il est possible d'utiliser le manque de protection de l'authentification et de l'intégrité des paquets afin de

mener une attaque par usurpation d'identité. Nous allons analyser un scénario d'attaque sur les vitesses de décollage reçues par les appareils via ACARS, ainsi qu'une manière d'exploiter les instructions de contrôle CPDLC.

Nous avons présenté une preuve de concept qui permet de forger de faux paquets ACARS afin de communiquer de manière illégitime avec des avions commerciaux, à l'aide d'une SDR et de Gnuradio. Le recours à ces outils nous permet de valider la possibilité d'une attaque grâce à une capacité intellectuelle et financière ainsi qu'une opportunité faible.

Enfin, nous avons utilisé des données ACARS collectées sur plusieurs semaines afin d'évaluer si l'adoption d'ARINC 823, une version sécurisée d'ACARS utilisée par l'US Air Force afin de communiquer avec les centres de contrôle civils, est viable d'un point de vue technique. Plus particulièrement, nous avons étudié l'impact sur la bande passante du recours aux méthodes cryptographiques utilisée par ARINC 823. Nos analyses démontrent que son adoption générale ne dégraderait pas de manière notable la qualité du service tout en augmentant considérablement la sécurité des communications par liaison de données.

ABSTRACT

The days when Archie League used flags to communicate with pilots are long gone. Modern communications protocol such as Datalink are now vital to air traffic control (ATC) operations. Thank to these new technologies which allow direct exchanges between embedded avionics components and control towers, air travel is now one of the safest modes of transportation.

Various protocols known as Datalink communications are now widely used by pilots, companies and controlers to share data directly over radio waves. Because they offer numerous advantages over classical voice communications, their adoption was fast and they are now mandatory on most of the controlled airspaces.

This extensive use of automated protocols has increased the attack surface of aviation towards deliberate cyberattacks that target the Datalink communication systems and the avionics. This potential threat is aggravated by the fast development and spreading of Software Defined Radios (SDR) and associated frameworks. Hackers are now able to listen and emit spoofed Datalink traffic that appear to come from ATC or from airborne aircraft, which may seriously interfere with aircraft and air traffic control operations. SDR technology is available at a very low cost and has a low barrier of entry in terms of technical knowledge. This would allow a vast number of motivated attackers to mount such attacks with relatively little risk of getting caught.

The first Datalink protocols originally deployed between 1980 and 1990 such as the Aircraft Communication Addressing and Reporting System (ACARS) and Controller Pilot Datalink Communication (CPDLC) are particularly vulnerable to spoofing attacks. Indeed, cybersecurity was not considered when they were designed. They do not incorporate any cryptographic protection of their integrity, authentication or condifentiality. Yet, they are still mandatory on most routes and now offer a prime target for hackers.

In this work, we first briefly make a brief state of the art of the current Datalink landscape. We describe how these protocols work and how they are being employed. We then conduct a threat analysis on several of them. Thanks to the interception of several Datalink packets, we developed some attack scenarios. They make it possible to take advantage of the lack of authentication in the ACARS and FANS1/A Datalink protocols in order to perform impersonation and message spoofing attacks. We complete our analysis by presenting them to currently flying airline pilots, which allows us to evaluate their potential impact on both efficiency of air traffic management and aircraft safety. In particular, we have successfully

identified an attack scenario where ACARS messages containing take-off speeds obtained from weight and balance calculations, could be modified by an attacker. Furthermore, we detailed how it is possible to send false information control using CPDLC.

We developed a proof-of-concept implementation of this attack with a Universal Software Radio Project (USRP) SDR using the Gnuradio framework. We kept at all time both the financial and intellectual ressources needed as low as possible in order to correctly assess which actors could launch this attack.

Finally, we use the ACARS traffic dataset gathered over a period of several weeks to study whether the adoption of ARINC 823, a secured version of ACARS used by the US Air Force to interact with civilian controllers, could be viable from a technical point of view, in particular with respect to bandwidth usage overhead. Our results show that its widespread adoption does not reprensent a problem in terms of quality of service while greatly enhancing the security.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

ACARS	Aircraft Communication Adressing and Reporting System
ACARS - MU	ACARS - Management Unit
ADS	Automatic Dependent Surveillance
AMS	ACARS Messaging Security
AMS	Aeronautical Mobile Satellite
AOC	Aeronautical Operational Control
ARINC	Aeronoautical Radio Incorporated
ATC	Air Traffic Control
ATN	Air Traffic Network
CDA	Current Data Authority
CNS/ATM	Communication Navigation Surveillance/Air-Traffic Management
CPDLC	Controller-Pilote Data Link Communication
CSMA	Carrier Sense Multiple Access
D-ATIS	Digital Automatic Terminal Information Service
DCL	Departure Clearance - *Autorisation de départ*
ECDH	Elliptic Curve Diffie Hellman
ECSDA	Elliptic Curve Digital Signature Aorithm
FANS	Future Air Navigation System
FMS	Flight Management System
HF	High Frequency - *Haute furéquence*
HMAC	Keyed-Hash Message Authentication Code
MAC	Message Authentication Code
MSK	Minimum Shift Keying
MTOW	Minimum Take Off Weight
NAA	National Aviation Authority - *Autorité aéronautique nationale*
NAT	North Atlantic Track
NRZI	Non Return to Zero Inverted
OACI	Organisation de l'aviation civile internationale - ICAO
OCL	Oceanic Clearance - *Autorisation Océanique*
OEM	Original Equipment Manufacturers - *Fabricant d'équipement d'origine*
POC	Proof Of Concept - *Preuve de concept*
SAM	Secure ACARS Message
SATCOM	Satellite Communication

TCAS	Traffic Collision Avoidance System
USAF	United States Air Force
USRP	Universal Software Radio Peripheral
VDL	VHF Data Link
VHF	Very High Frequency

CHAPITRE 1 INTRODUCTION

1.1 Historique du contrôle et des communications aériens [1]

Deux années seulement séparèrent les tentatives de quatre pionniers qui changeraient à jamais le regard que portent les hommes sur le ciel. Le 12 décembre 1901, Guglielmo Marconi réussit à l'aide de son assistant à envoyer la lettre «s» en code Morse à travers l'Atlantique. C'est la force du vent qui lui permit de déployer une antenne attachée à un cerf volant, nécessaire à la réalisation de sa performance scientifique. La même force qui, comme un présage de l'étroite relation qui lierait à jamais ces deux domaines, autorisa les frères Wright à réaliser leur premier vol motorisé en 1903.

Les pionniers de l'aviation ne pouvaient compter que sur leurs sens et leur instinct pour affronter un ciel jusqu'alors indompté. Les premières applications des communications sans fil dans les aéronefs remontent à la Première Guerre mondiale pendant laquelle certains appareils furent équipés de systèmes de communication qui permettaient aux pilotes d'observer les lignes ennemies et d'informer les troupes alliées sans avoir à revenir au sol grâce à des messages en morse. Le mariage était consommé et l'aéronautique ainsi que les radiocommunications adopteraient un destin commun.

Les technologies des deux domaines ont connu des avancées majeures simultanées et les pilotes aux commandes d'avions de plus en plus rapides et performants purent compter sur des systèmes sans fil pour définir les routes aériennes, se repérer dans le brouillard, etc. La visibilité ne fut alors plus un facteur nécessaire au bon déroulement des vols. La fameuse maxime du «voir et être vu» devint caduque et un besoin de contrôle du trafic aérien apparut.

Le premier contrôleur aérien était Archie League, qui «guidait» les appareils au décollage et à l'atterrissage de l'aéroport de Saint-Louis dans le Missouri à l'aide de simples drapeaux en 1929. Ces systèmes de fortune furent rapidement supplantés par les radios et les ordres de navigation adressés aux appareils furent bientôt transmis directement aux aéronefs concernés via la voix grâce à l'apparition de la radio moderne.

La Deuxième Guerre mondiale fut, plus que tout autre conflit, un affrontement technologique. Suite à la signature de l'armistice, de nombreuses inventions autrefois dédiées au domaine militaire furent adaptées au monde civil qu'elles pouvaient dorénavant servir. Le contrôle du trafic aérien, jusqu'alors assuré par des observateurs terrestres s'effectuerait désormais via

1. Les faits suivants sont en majorité tirés des livres «Principles of Avionics, Seventh Edition» (Helfrick, 2012) et «Fundamentals of Air Traffic Control» (Nolan, 2011)

les systèmes RADAR développés par les forces alliées pour se prémunir des bombardements allemands.

Cette période vit également l'apparition du premier avion commercial à réaction, le Boeing-707 qui révolutionna le transport de passager et permit d'augmenter une fois de plus le volume des appareils empruntant les routes aériennes. Pour faire face aux nombreux défis de coordinations des services de contrôle aérien entre nations, une organisation internationale de régulation de l'aviation fut créée en 1947 : l'Organisation de l'aviation civile internationale - OACI. Au Canada, au niveau territorial, c'est Transport Canada qui est encore aujourd'hui chargé de la supervision de l'aviation civile. Transport Canada travaille en relation étroite avec d'autres autorités, telles que la Federal Aviation Agency - FAA créée en 1958, son équivalent américain.

Rapidement, les fréquences radio classiques dédiées aux échanges via la voix se révélèrent insuffisantes et il apparut vital de trouver de nouveaux moyens de communication. Afin de permettre aux aéronefs d'échanger directement avec les systèmes désormais numériques des tours de contrôle, des liaisons de donnée entre les *Air Trafic Control Unit* - ATCU et les appareils furent mises en place. Le terme de liaison de données, également appelées Datalink, désigne l'ensemble des techniques employées afin de transmettre sur des ondes radio des données utiles entre tous les acteurs impliqués dans un vol (contrôleur, pilote, compagnie,etc.).

Les liaisons de données permettent dorénavant aux compagnies aériennes de communiquer directement avec leurs appareils à des fins opérationnelles (communications *Airline Operational Control* - AOC). Dans le cadre du contrôle du trafic aérien (communications *Air Traffic Control* - ATC), elles présentent de nombreux avantages sur les opérations radio «classiques». En effet, le recours à des informations textuelles reçues par les pilotes et les contrôleurs simplifie grandement les échanges d'information tout en réduisant drastiquement le risque d'une mauvaise interprétation. Les bandes de fréquences sont mieux exploitées et il est possible de surveiller et d'aiguiller plus d'appareils simultanément (Transport Canada, 2016). Enfin, le problème de «stuck mic» qui survient lorsqu'une radio émet accidentellement en continu et monopolise la fréquence disparaît. Les paquets et les protocoles utilisés diffèrent d'une technologie à l'autre, mais le principe de fonctionnement ainsi que le contenu des messages restent sensiblement le même. On peut distinguer trois types principaux de liaisons de données aux usages variés et complémentaires.

1.2 Classification des communications par liaison de données

Le premier système de liaison de données est apparu en 1978 et fut appelé *Aircraft Communication Addressing and Reporting System* - ACARS (ARINC, 2016). Il était l'initiative d'une organisation de normalisation désormais privée appelée ARINC. Encore utilisé aujourd'hui, il permet l'envoi d'informations brèves (220 octets maximum) via les ondes VHF, HF ou satellites. Le système ACARS fut déployé sur de nombreux appareils au cours des années 80.

Peu de temps après, l'OACI mit en place un comité chargé de trouver des solutions adaptées à l'évolution du paysage aéronautique, appelé *Future Air Navigation System* - FANS (ATNP Working Groups, 1999). Pour la première fois, les bases d'un système de surveillance uniformisé au niveau mondial furent posées et un plan de déploiement en plusieurs phases fut rédigé. Ce concept est connu sous le nom de CNS/ATM (Communication Navigation Surveillance/Air Traffic Management), et repose en grande partie sur le recours aux liaisons de données et aux communications satellites. Fruit des recommandations exprimées par ce comité, une évolution des réseaux de liaison de données, appelée *VHF Data Link- FANS 1/A* - VDL apparu au début des années 1990. Les premiers systèmes compatibles FANS furent développés par Airbus et Boeing puis utilisés à partir de 1995. Ils sont encore aujourd'hui en cours de déploiement dans le monde entier. Ils présentent des débits bien supérieurs à ceux permis par ACARS et autorisent l'utilisation de protocoles plus complexes et performants.

Plus récemment, devant l'utilisation croissante des liaisons de données afin de permettre d'interfacer plus facilement les systèmes digitaux des tours de contrôle et des aéronefs, l'OACI a émis le souhait de mettre en place un réseau mondial dédié aux liaisons de données pour le contrôle du trafic aérien baptisé par la suite *Air Traffic Network* - ATN (ARINC Working Group M, 2000). Ce dernier fait partie de la deuxième phase du FANS et est une des structures vitales à la mise en place du CNS/ATM. Le réseau ATN doit à terme offrir des fonctionnalités plus variées que les liaisons de données de génération précédente sur un réseau unique pour toutes les communications AOC et ATC. Il vise à remplacer définitivement d'ici 2025 toutes les technologies de liaison de données déjà en place (Boeing, 2016).

Les trois types de liaison de données que nous venons de décrire coexistent aujourd'hui. Un mélange complexe de technologies en résulte donc. Les différentes utilisations qui sont faites de chacune sont résumées dans le tableau 1.1.

Tableau 1.1 Utilisation des liaisons de données pour les messages AOC et ATC (FAA, 2012)

	AOC	**ATC**
ACARS	• Messages en texte clair	• Communications ATC • Autorisations de départ - DCL • Autorisations océaniques - OCL • Informations Météo - D-ATIS
FANS 1/A		• ADS - C • Communications ATC • CPDLC
ATN (Futur)	• Communications sur IP	• Communications ATC • CPDLC sur ATN

1.3 Problématique

1.3.1 Failles des protocoles de liaison de données

Lors des vols commerciaux classiques, les aéronefs traversent toujours une période de croisière appelée *En route*. Pendant ces phases de vol, comme la traversée de grandes étendues océaniques, de nombreuses contraintes rendent caduque l'utilisation des techniques classiques pour la surveillance et le contrôle des appareils. Il est par exemple tout à fait impossible d'avoir recours à des informations RADAR à cause de la portée limitée des stations présentes sur les côtes. En outre, les ondes VHF ne permettent que des communications en ligne de vue. Ainsi, seuls les ondes HF et les réseaux satellites permettent de garder le contact avec les avions au-dessus des océans, mais ces derniers offrent une bande passante limitée. Il n'est alors plus pertinent de systématiser le recours à la voix pour les opérations de contrôle aérien, car les fréquences seraient rapidement saturées. Certains protocoles de communication plus récents comme ACARS et FANS1/A sont donc privilégiés, voir même systématisés dans certaines zones empruntées par les appareils en route (FAA, 2012). En outre, comme nous l'avons déjà vu, l'utilisation des instructions reçues via liaison de données supprime les problèmes d'interprétation des communications orales qui peuvent parfois être mal comprises, et permet d'armer le système de navigation immédiatement après vérification.

Le recours à la liaison de données permet d'assurer la disponibilité en tout temps des canaux de communication aéronautiques classiques. La réception des messages ACARS et FANS-1 se doit d'être fiable puisque tout le trafic transocéanique repose sur les liaisons de données. Ces systèmes performants garantissent un niveau d'automatisation toujours plus élevé au sein de l'écosystème aérien résultant en une meilleure gestion des données, de l'espace aérien, tout en garantissant une sécurité accrue.

En parallèle, la surface d'attaque des systèmes aéronautiques basés sur les liaisons de données a été considérablement élargie. Si l'utilisation des systèmes numériques ne pose pas de problème en soit, l'implémentation qui en a été faite ouvre de nouvelles opportunités (Bresteau et al., 2018). En effet, les différents systèmes critiques (contrôle de l'appareil, FMS, navigation) sont maintenant directement reliés à des systèmes accessibles depuis l'extérieur que sont les communications Datalink. Les problématiques de sécurité informatique ne sont considérées que depuis peu dans le développement des différents protocoles utilisés par les avions commerciaux. Ainsi, les systèmes en place présentent de nombreuses failles. Si l'exploitation de ces dernières nécessitait encore il y a quelques années des connaissances et des moyens financiers importants, cette menace potentielle est d'autant plus forte que de nombreux systèmes à faible coût comme des Software Defined Radio (SDR) ainsi que les environnements de développement associés sont désormais accessibles au grand public. Les avions commerciaux font donc dorénavant face à diverses menaces qu'il convient de définir.

1.3.2 Quels sont les acteurs de menace ?

Plusieurs discours existent concernant la sécurité des liaisons de données. Certains acteurs prétendent avoir réussi prendre pleinement le contrôle d'un appareil en exploitant des failles de sécurité (Perez, 2015). Ceci contraste fortement avec l'absence de développement de solution rétrocompatibles de sécurisation des communications Datalink autre que sur ACARS. Dans ce travail, nous allons évaluer de manière objective et scientifique quelle est la situation de la sécurité des protocoles de communications par liaison de données. Plus particulièrement, nous allons détailler de quelle manière il est exactement possible de compromettre, ou non, un appareil.

Nos recherches se basent sur le recours à des données connues et disponibles sur Internet. L'assurance qu'à aucun moment nous n'avons recours à une source de données secrète ou à un niveau élevé d'expertise nous permet de nous assurer que nos recherches seront valables pour des acteurs ayant une opportunité moyenne ou faible. Il en sera de même pour les moyens financiers. Les différents résultats que nous avons obtenus utilisent du matériel facilement accessible et bon marché. Nous sommes ainsi confiants dans la véracité de l'analyse de risque que nous faisons sur les communications Datalink.

Une analyse de risque complète comme celle qui sera menée dans de ce mémoire doit également considérer quels sont les potentiels assaillants des systèmes de communications des avions commerciaux. Nous mettrons de côté tous les acteurs internes au fonctionnement de l'aviation commerciale (contrôleurs, pilotes, mécaniciens...). Ces derniers disposent de nom-

breuses méthodes d'action afin de compromettre la sécurité des vols. La surveillance de leurs actions nécessiterait des méthodes complexes qui sont au-delà du périmètre de ces travaux.

Plusieurs études comme celle menée par (Arasly, 2005) et (Lam et al., 2017) portent déjà sur les acteurs d'attaque potentiels. Si le risque actuel semble faible, un certain intérêt de la part de potentiels agents de menace émerge quant au recours à des cyberattaques visant des systèmes aéronautiques.

1.3.3 Sécurisation des communications Datalink

Certains standards de sécurisations sont déjà disponibles et offrent des solutions considérées robustes. C'est par exemple le cas d'ACARS Message Security - AMS, connu sous le nom d'ARINC 823. S'il adresse les failles de sécurité connues du système de communications ACARS, son utilisation est aujourd'hui limitée aux appareils militaires. En effet, AMS a été développé pour permettre à l'U.S. Air Force de garantir un accès aux systèmes de contrôle civils tout en garantissant la confidentialité des échanges de ses aéronefs. Son utilisation dans un contexte purement commercial n'est pas évidente, car les problématique de sécurité et de performance sont différentes. Sa viabilité pour répondre aux besoins des avions de transport de passagers reste à être prouvée.

Les différentes techniques de cryptographie classiques, qui permettent la mise en place de session de communications sécurisées, nécessitent des échanges d'informations supplémentaires entre les différents utilisateurs. Ceci a pour effet d'augmenter l'utilisation faite des bandes de fréquences disponibles, ce qui risquerait de les saturer. La bande passante à disposition des appareils en vols transcontinentaux est limitée, car les communications Datalink reposent alors uniquement sur des hautes fréquences et sur des communications satellites. Comme la résilience des systèmes actuels face à l'utilisation intensive de mesures cryptographiques n'a pas encore été démontrée, il convient de déterminer quel est le risque de congestion des réseaux sur lesquels transitent les paquets de liaison de données.

1.4 Objectifs et questions de recherche

L'objectif des travaux menés au cours de cette recherche est d'évaluer les risques liés à une attaque active sur les communications par liaison de données, ainsi que d'évaluer la viabilité de l'adoption des contre-mesures déjà disponibles. Afin d'atteindre ce but, nous avons tenté de traiter les questions de recherche suivantes :

- **Q.1.** Quelles sont les failles des communications de liaison de données aéronautiques ?

- **Q.2.** Jusqu'à quel point une attaque active sur ACARS et/ou FANS 1/A peut-elle influencer le bon déroulement d'un vol commercial ?

- **Q.3.** Quelle est la difficulté de mener une attaque active sur les communications aériennes par liaison de données ? Quels sont les requis techniques minimums afin d'intercepter et d'émettre des messages de contrôle aérien ?

- **Q.4.** Est ce que l'utilisation étendue d'AMS est viable comme moyen de protection des échanges Datalink tant sur le plan technique qu'opérationnel ?

- **Q.5.** Quel serait l'impact sur les réseaux actuels du recours à des solutions cryptographiques du type d'AMS ?

1.5 Plan de mémoire

Afin de cerner au mieux les problèmes rencontrés, le chapitre 2 présente de manière détaillée les différentes technologies et acteurs impliqués dans le contrôle du trafic aérien. Le chapitre 3 résume toutes les propositions de sécurisation des liaisons de données avancées par la communauté scientifique ainsi que les industriels de l'aéronautique.

Une analyse de risque poussée est menée dans le chapitre 4. Elle permet de définir les objectifs de sécurité à tenter de maintenir en priorité et détaille des scénarios d'attaques crédibles sur les communications par liaison de données. L'attaque active menée en milieu expérimental décrite dans le chapitre 5 tente de valider les différentes hypothèses soulevées par l'étude préliminaire et l'analyse de risque.

Le chapitre 6 est consacré à l'étude de faisabilité de l'adoption de communications par liaison de données sécurisée. Nous détaillerons jusqu'à quel point la résilience des réseaux déjà en place permet l'utilisation des solutions cryptographiques déjà standardisées et avanceront des pistes d'amélioration des standards déjà en place.

Enfin, un résumé des différents résultats exposés au cours de ce mémoire sera exposé dans le chapitre 7, et les différentes réponses aux questions de recherches proposées seront clarifiées. Enfin, des perspectives de recherche futures seront proposées afin d'identifier les prochains défis de la sécurisation des protocoles de communication aéronautiques.

CHAPITRE 2 PRINCIPES FONDAMENTAUX DU FONCTIONNEMENT DES LIAISONS DE DONNÉES

2.1 Acteurs impliqués dans le contrôle du trafic aérien

De nombreux acteurs sont impliqués dans la rédaction et l'application des règles du contrôle du trafic aérien. La compréhension du rôle que joue chacun d'entre eux est d'autant plus complexe que certains agissent au niveau domestique là ou d'autres sont impliqués dans une collaboration internationale. L'Organisation de l'aviation civile internationale - OACI, rattachée aux Nations Unies, a été créée à la fin de la Deuxième Guerre mondiale et a pour objectif d'établir des normes permettant de définir des standards mondiaux dans le domaine du transport aérien. En Europe, c'est l'European Aviation Security Agency - EASA qui encadre la coopération entre les différents pays de l'Union européenne en ce qui concerne le contrôle du trafic aérien uniquement. Les entités nationales sont regroupées sous le nom de *National Aviation Authority* - NAA. La *Federal Aviation Administration* - FAA ou encore la Direction Générale de l'Aviation Civile - DGAC sont les agences en charge des règles du transport de passagers aéroporté respectivement aux États-Unis et en France. Dans certains pays (comme le Canada avec l'agence NAV CANADA), le contrôle du trafic aérien ainsi que sa réglementation sont confiés à des compagnies privées.

Toutes ces autorités, et plus particulièrement l'EASA et la FAA, rédigent des standards en coopération avec les constructeurs privés, ce qui permet une meilleure intégration des équipements avioniques. De nombreuses technologies qui seront détaillées dans ce document proviennent des efforts de constructeurs privés qui développent leurs propres solutions. C'est par exemple le cas d'Aeronautical Radio, Incorporated - ARINC, créée en 1929. Il s'agit à l'origine d'une entreprise détenue par les plus grosses compagnies aériennes et certains manufacturiers aéronautiques aux États-Unis et a pour objectif principal la rédaction des principaux standards de communications utilisés par les aéronefs. Il s'agit aujourd'hui d'une entreprise privée détenue exclusivement par Rockwell Collins. Elle est à l'origine de nombreux standards concernant les liaisons de données qui seront utilisées dans ce mémoire. Les normes développées par ARINC permettent de grandement faciliter l'interopérabilité des équipements présents dans les avions (Helfrick, 2012). Elles définissent les paramètres nécessaires à l'utilisation d'équipements de communication au sein des appareils et vers l'extérieur. Tant qu'un matériel utilisant un standard ARINC a les bonnes informations en entrée, il donnera en sortie ce qui est attendu de lui. Cela permet l'interopérabilité des équipements d'un fabricant à l'autre, tant que les règles d'interfaçage définies par ARINC sont respectées.

L'action cumulée et collaborative de ces nombreuses institutions permet en tout temps d'assurer le bon déroulement des opérations ATC. Ceci n'est possible que grâce à l'utilisation coordonnée de nombreuses technologies sans fil. Afin de saisir au mieux le fonctionnement complexe des liaisons de données, il convient d'en expliciter les modalités d'utilisation en détail.

2.2 Utilisation des liaisons de données

Le terme générique "liaison de données" utilisé en aéronautique regroupe en fait de nombreuses technologies et liaisons de données indépendantes au fonctionnement ainsi qu'aux utilisations variées (ICAO, 2013). Les premières furent les liaisons ACARS standardisées en 1978 (ARINC, 2016). Entre 1991 et 1996, l'apparition des recommandations Future Air Navigation System - FANS a vu la mise en service des réseaux VDL (VHF Data Link) augmentant considérablement les performances du système et donc ses utilisations potentielles. Depuis 2000, les composantes avioniques ACARS classiques ont été modifiées afin de pouvoir utiliser les stations VDL qui offrent de meilleures performances et une couverture accrue. En dehors des zones de couverture du VDL, les composantes avioniques basculent sur le fonctionnement classique à faible débit de la liaison ACARS.

L'utilisation de la liaison de données pour des opérations de contrôle du trafic aérien remonte à la mise en place d'ACARS, lors des manœuvres pour lesquelles le délai de réponse n'est pas un facteur critique. C'est par exemple le cas des autorisations océaniques, appelées OCL, qui permettent à un appareil à lorsqu'il le nécessite d'emprunter une route océanique à une vitesse et une altitude précise. Des autorisations similaires de départ, appelées DCL, permettent aux pilotes de recevoir la permission d'effectuer un départ lors de vols aux instruments. Par la suite, avec l'apparition de technologies plus performantes, le recours aux technologies reposant exclusivement sur les réseaux VDL tel que le Controller-Pilot Datalink Communications - CPDLC s'est grandement démocratisé. En effet, Boeing a mis en place pour la première fois le système FANS-1 dans ses Flight Management System - FMS, suivi par Airbus avec un système équivalent nommé FANS-A. Ces technologies continuent d'évoluer selon les recommandations du comité FANS de l'OACI. Le terme FANS1/A définit donc maintenant l'ensemble des protocoles qui transitent via le réseau VDL (tels que CPDLC ou ACARS sur VDL). La figure 2.1 détaille les zones d'implémentation et d'utilisation des diverses liaisons de donnée dans le monde entier.

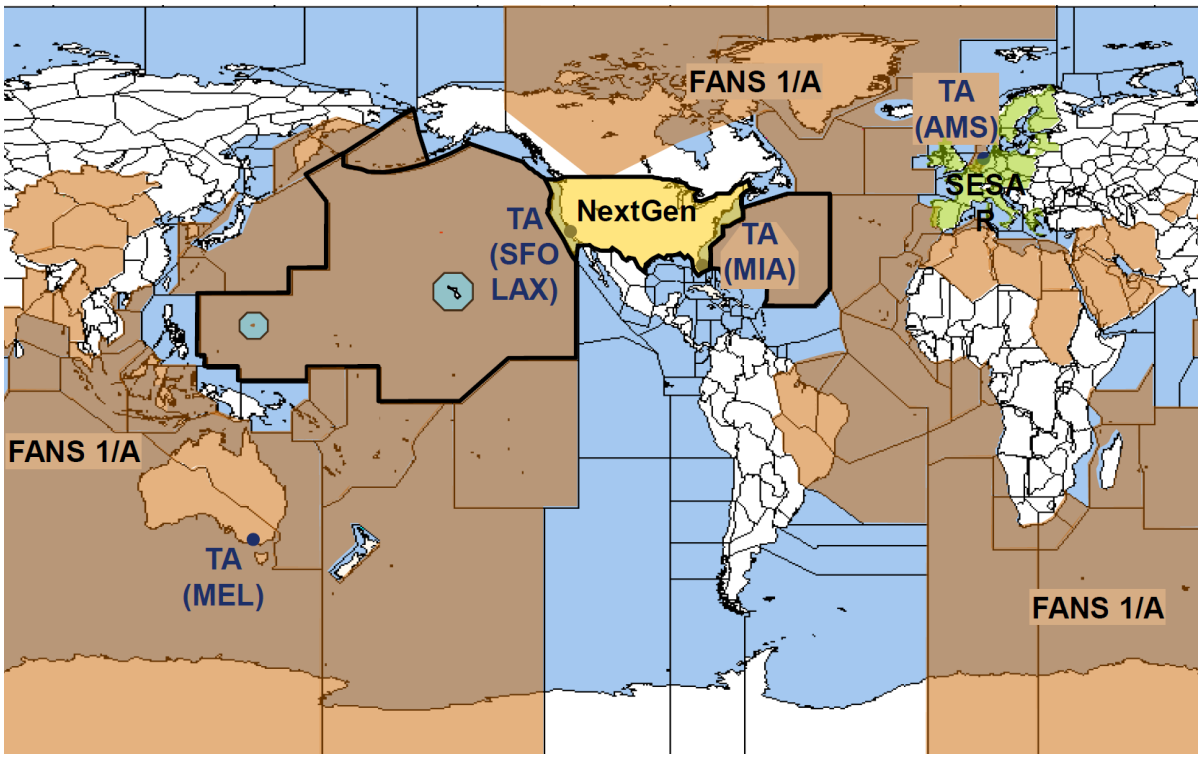


Figure 2.1 Zones d'utilisation des liaisons de données. Les zones Tailored Arrival - TA permettent aux appareils de recevoir leur plan de descente directement via liaison de donnée. Le NextGen représente l'ensemble des protocoles devant succéder à FANS1/A aux États-Unis et le SESAR est son équivalent Européen. Les deux adopteront des technologies similaires afin de permettre une meilleure interopérabilité des équipements. (Kraft, 2009)

La variété des réglementations ainsi que les spécificités liées aux opérateurs des réseaux sur lesquels s'appuient les liaisons de données créent des systèmes de communication très hétérogènes. Dans un souci de clarté, nous tenterons d'expliciter le fonctionnement des communications transatlantiques sur la zone du vol du North Atlantic Track - NAT, qui représente à elle seule environ la moitié des échanges FANS1/A dans le monde (Kraft, 2009). Dans cette zone, la liaison de données permet d'assurer toutes les opérations de contrôle aérien ainsi que de fournir des rapports de position pour pallier au manque de couverture RADAR.

2.3 Caractéristiques ACARS

Parmi les différentes technologies utilisées pour les liaisons de données, ACARS est la plus ancienne. L'idée d'une liaison de données a été proposée par ARINC en 1978 et les détails de son fonctionnement sont explicités dans la norme (ARINC, 2016). Les liaisons ACARS

permettaient lors de leur déploiement en 1978 des communications allant jusqu'à 2.4 kbit/s sur des ondes VHF (SITA, 2016).

Elle permet une communication bidirectionnelle entre les systèmes avioniques, les systèmes au sol des tours de contrôle et les compagnies aériennes. Le système ACARS, bien qu'à l'origine limité aux bandes radio VHF peut utiliser les liaisons satellites comme support physique et les hautes fréquences HF. Il s'agit d'un protocole orienté caractère relativement simple. Aucun *handshake* n'est nécessaire à l'établissement d'une session et il suffit de fournir correctement l'adresse d'un utilisateur pour que le message lui soit adressé tant qu'il est à l'écoute sur la bonne fréquence. Afin d'éviter et de détecter les collisions, la couche physique est partagée grâce au protocole du Carrier Sense Multiple Access (CSMA).

Pour fonctionner, ACARS nécessite des équipements au sol (un simple micro-ordinateur connecté à un émetteur HF ou VHF) ainsi que des équipements embarqués (ACARS management unit, *control display unit*, récepteur VHF/HF). La structure des paquets est toujours la même quel que soit le message et est donnée dans le tableau 2.1.

Tableau 2.1 Structure des paquets ACARS - (ARINC, 2016)

CHAMP	**LONGUEUR (Octets)**	**CONTENU (hexa)**
Pre Key	20	0xFF...2B2A1616
Start of Heading	1	0x01
Mode	1	Arbitraire
Address	7	Arbitraire
Technical Acknowledgment	1	Arbitraire
Label	2	Arbitraire
Uplink/Downlink Block Identifier	1	Arbitraire
Start of Text	1	0x02
Text	220	Arbitraire
Suffix	1	0x03 ou 0x17
Block Check Sequence (BCS) - CRC16 Kermit	2	Arbitraire
BCS Suffix	1	0x7F

Afin de synchroniser le récepteur, une *Pre Key* est utilisée. Il s'agit d'une suite de 16 caractères "1" (0xFF) suivis de "+*" (0x2B2A) puis de deux caractères SYN (0x16). Le champ d'adresse permet d'identifier l'aéronef ou les infrastructures au sol concernées par le message envoyé. Les messages downlink (air vers le sol) contiennent l'immatriculation de l'appareil émettant le paquet. Les messages uplink contiennent l'identifiant unique attribué par l'OACI à l'émetteur. Le champ *label* permet de déterminer l'objectif du message (communication AOC, ATC, ATIS, rapport météo, clairance, etc.). Enfin, le champ *text* contient la charge utile du paquet

qui s'affichera sur les équipements à la réception d'un message. Si le message est plus long que 220 caractères, le paquet est découpé et le caractère de suffixe transmis sera *End of Transmitted Block* - ETB. Lorsque le texte touche à sa fin ou lorsqu'il s'agit du dernier bloc d'un long message, le caractère de suffixe sera *End of Transmission* - ETX.

Une fois que tous les champs du paquet sont remplis, le message est encodé selon la méthode *Non Return to Zero Inverted* - NRZI. Si le bit envoyé est un "1", on procède à un changement d'état, si le bit envoyé est un "0" il ne se passe rien. Un exemple de NRZI est donné dans la Figure. 2.2

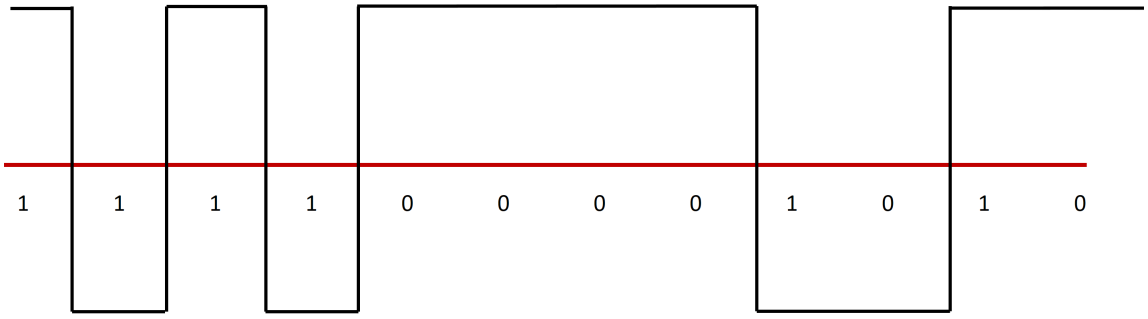


Figure 2.2 Encodage NRZI

L'encodage effectué, le signal est modulé en MSK (Minimum Shift Keying). Il s'agit d'une modulation de fréquence utilisant deux "pseudo porteuses" de 1200 et 2400 Hz, appelées respectivement *L.Tone* et *H.Tone*. Ces fréquences dépendent directement des caractéristiques de la MSK et sont imposées par le débit de 2400 bits par seconde d'ACARS. Un changement de bit est traduit par une tonalité de 1200 Hz et une tonalité de 2400 Hz indique qu'il n'y a pas eu de changement de bit. Il convient également de noter que la phase du signal est continue lors d'une modulation MSK, ce qui permet d'identifier rapidement le bit transmis - figure 2.3. Le comportement d'une trame modulée en MSK est observable la Figure 2.4.

De nombreuses bandes de fréquences sont attribuées à l'utilisation d'ACARS à la fois en très hautes (VHF) et hautes fréquences (HF) ainsi qu'en communications par satellite (SATCOM). En revanche, quelle que soit la couche physique employée, le signal en bande de base restera exactement le même.

2.4 Caractéristiques FANS1/A

Afin de permettre une amélioration des performances de la liaison de données et des services proposés, le VDL Mode 2 a été entièrement défini par l'OACI (UASC, 2017). Le réseau

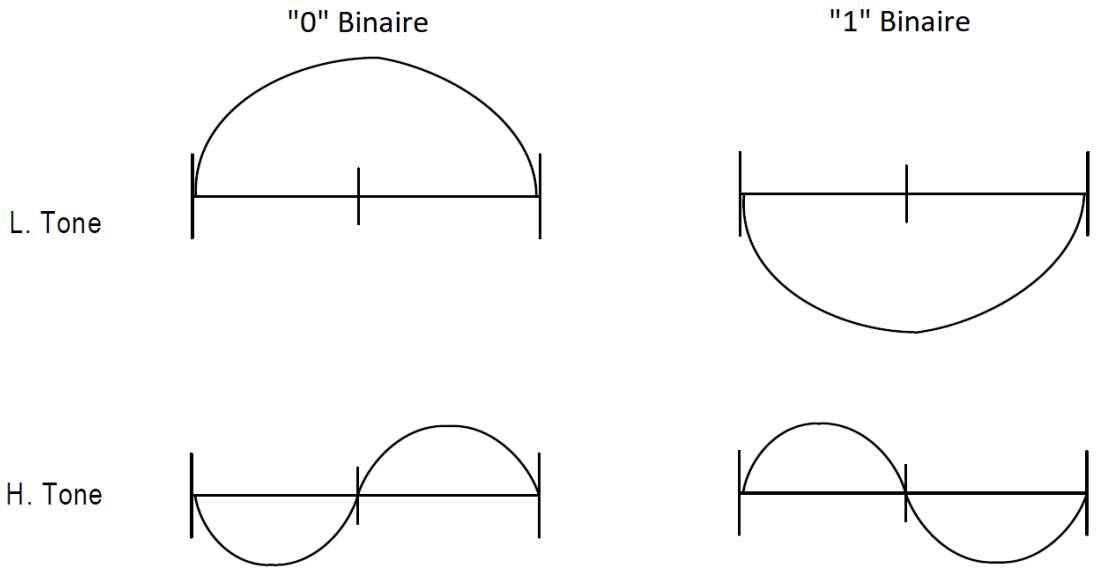


Figure 2.3 Signaux binaires modulés en MSK (ARINC, 2016)

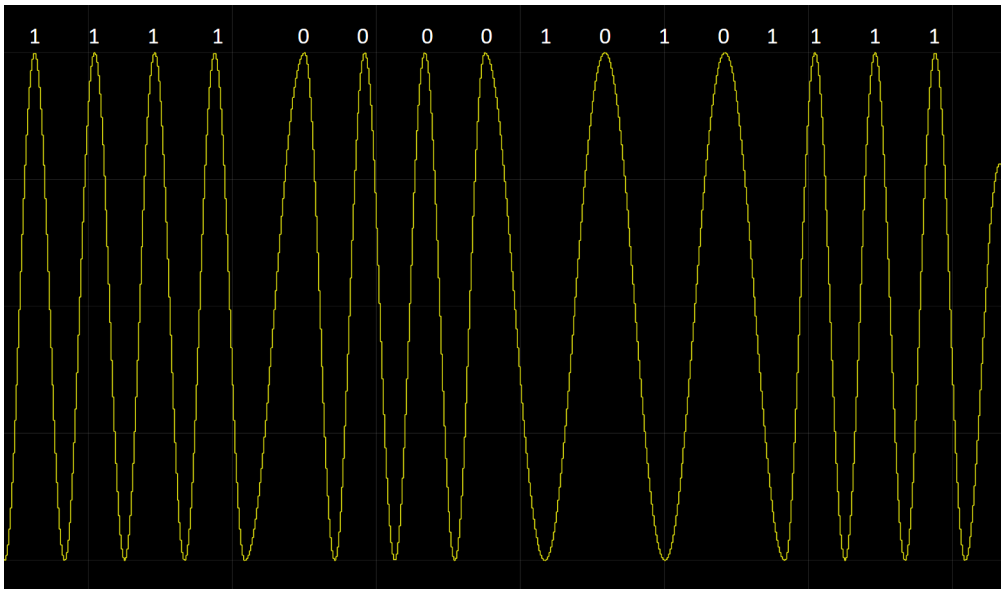


Figure 2.4 Signal MSK - Simulation Simulink

VDLM2 est apparu au début des années 90 (SITA, 2016) et permet des communications bien plus rapides qu'ACARS (environ 31.5 kbit/s). Les nombreux services proposés par FANS1/A reposent dorénavant sur ce dernier. Les deux fournisseurs d'accès au réseau VDLM2 sont ARINC et la Société Internationale de Télécommunications Aéronautiques - SITA. Ces deux

acteurs mettent à disposition des compagnies aériennes l'infrastructure physique nécessaire aux communications Datalink. Aujourd'hui, cette liaison de données sert entre autres de support aux communications afin de permettre des opérations de contrôle classiques.

Le recours aux protocoles FANS1/A tel que CPDLC, permet de réduire les risques de congestion du réseau tout en se basant sur des ordres de contrôle classiques et régulés (ICAO, 2013). Sur le long terme, VDLM2 remplacera probablement toutes les communications ACARS, mais ces dernières restent aujourd'hui encore largement utilisées. Afin de faciliter la transition entre les deux technologies, les spécifications ACARS les plus récentes, (ARINC, 2016) permettent son fonctionnement directement sur les réseaux VDL tout en conservant la forme des paquets ARINC 618. Afin de pouvoir atteindre les performances requises, les caractéristiques de haut et bas niveaux de cette liaison de données sont radicalement différentes de celles de son prédécesseur (Lundström, 2016).

Tableau 2.2 Structure des trames AVLC - (Lundström, 2016)

Champ	**Longueur**
FLAG	1
Destination	4
Source	4
Contrôle	1
Information	N
Frame Check Sequence	2
FLAG	1

La bande de fréquence VHF attribuée au VDLM2 est située entre 117.975 et 137 MHz, qui sont également utilisée pour la voix dans certaines zones. Les trames sont séparées en deux parties, une séquence d'entraînement, détaillée dans la figure 2.5 suivie d'une trame AVLC (Aviation VHF Link Control) - Figure 2.2.

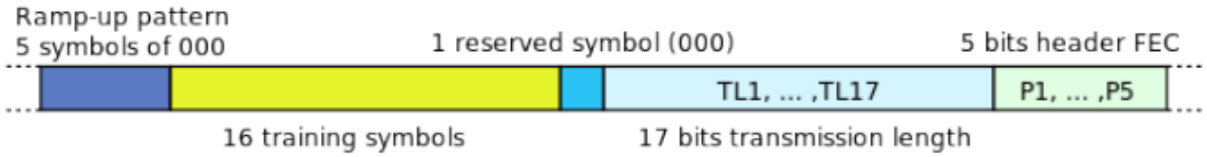


Figure 2.5 Séquence d'entraînement VDL (Lundström, 2016)

L'encodage effectué, le signal est modulé en D8PSK (Differential 8-Phase Shift keying), une modulation de phase avec un code de Gray donné sur la figure 2.7.

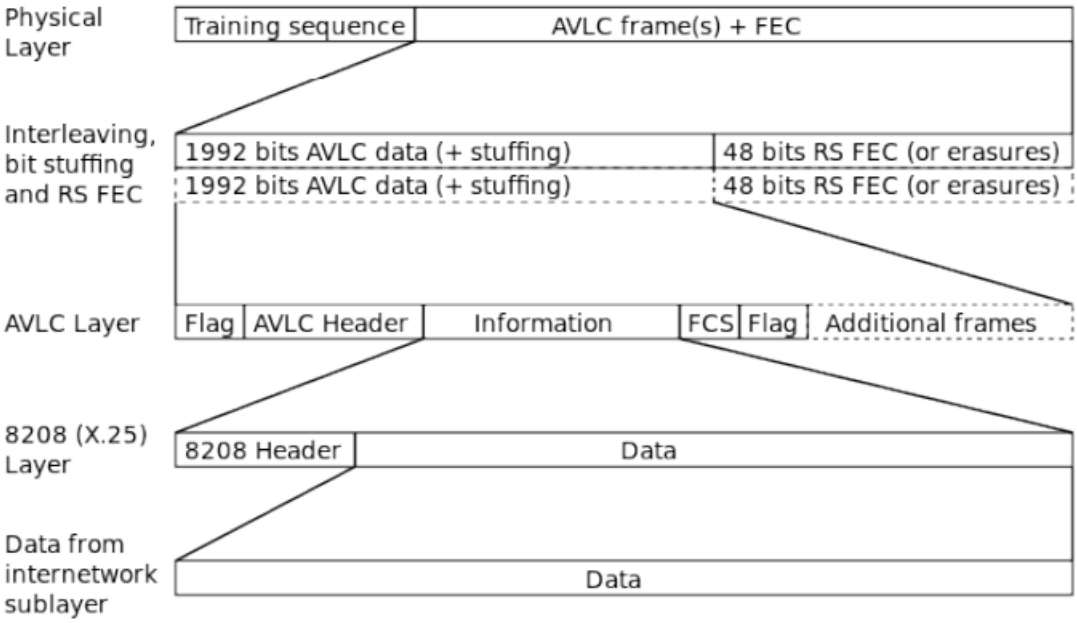


Figure 2.6 Paquet VDML2 complet (Lundström, 2016)

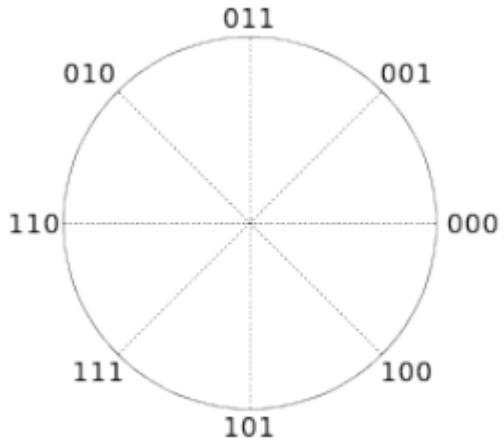


Figure 2.7 Constellation D8PSK (Lundström, 2016)

En plus de présenter des caractéristiques techniques différentes d'ACARS, les procédures d'établissement de communications sont relativement plus complexes. Un appareil ne peut communiquer qu'avec un seul centre de contrôle, appelé CDA (Current Data Authority) et possède une connexion inactive avec le prochain centre de contrôle qu'il devra contacter, le NDA (Next Data Authority) (ICAO, 2013). Les connexions sont initiées par un *logon* de la part de l'avion, auquel le centre de contrôle concerné doit répondre. Suite au logon, l'ATC

envoie un message *connection request* l'appareil répondra par un *confirm*. Ce mécanisme de handshake n'est pas présent dans les protocoles Datalink antécédents.

Ce sont les ATSU qui ont la pleine responsabilité d'*initier*, *transférer* ou de *mettre fin* à toutes les communications VDLM2 avec un appareil. Les messages sont généralement envoyés par l'ATC en premier puis confirmés par l'appareil en vol. Dans chacun des cas, des contrôles procéduraux sont mis en place afin de faire en sorte qu'un appareil soit en tout temps en contact avec le centre de contrôle de l'espace aérien dans lequel il évolue et chaque session est initiée ou terminée par le handshake que nous venons de décrire. Le cycle de vie d'une communication CPDLC sur VDLM2 est détaillé dans la figure 2.8.

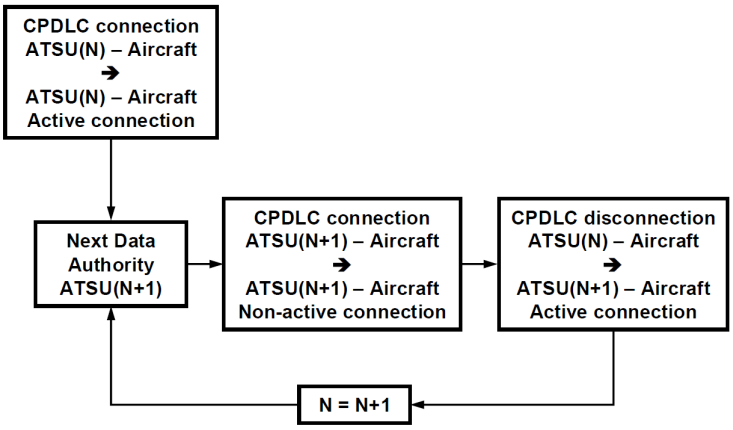


Figure 2.8 Cycle de vie d'une communication CPDLC (ICAO, 2013)

CHAPITRE 3 ÉTAT DE L'ART SUR LA SÉCURITÉ DES PROTOCOLES DE LIAISON DE DONNÉES

3.1 Menaces potentielles actuelles

La sécurité informatique s'évertue à protéger en tout temps trois objectifs principaux : *la confidentialité*, *l'intégrité* et la *disponibilité* des systèmes ainsi que des données. En plus de ces trois objectifs, il convient de mettre l'emphase sur une notion qui sera particulièrement sensible dans le cas des liaisons de données : l'*authenticité* des messages transmis. Les différentes menaces qui pèsent sur les liaisons de données relativement à chacun de ces objectifs ont déjà été traitées de manière intensive dans la littérature (Olive, 2001) (Sampigethaya et al., 2011) (Storck, 2013). Les appareils commerciaux reposent de plus en plus sur des systèmes informatiques et de réseaux de communications qui, au même titre que les réseaux de communications grand public (comme Internet) présentent en puissance des failles exploitables. Nous allons tenter au cours de cette partie d'évaluer les risques qui pèsent sur les liaisons de données en termes de *confidentialité*, de *disponibilité*, d'*intégrité* et d'*authenticité*. Les deux dernières notions citées, bien que proches et souvent regroupées sous la même terminologie, sont ici volontairement distinguées par souci de clarté.

3.1.1 Confidentialité

Assurer la *confidentialité* des messages des liaisons de données consisterait à faire en sorte que seuls les acteurs impliqués dans les opérations d'exploitation d'un avion commercial aient accès au contenu des messages transmis. Néanmoins, à cause de la nature même du support physique, c'est-à-dire des ondes radio, il est impossible d'empêcher l'accès aux échanges. N'importe quelle personne disposant d'une SDR (Software Defined Radio) ou de matériel de communication aéronautique dédié est en mesure d'intercepter des messages de liaison de données. La seule contre-mesure efficace serait la mise en place de systèmes de chiffrement, qui n'existe pas dans le cas des communications ACARS et FANS1/A. Dans le premier cas, les messages interceptés sont directement interprétables, car les paquets contiennent le texte en clair. Les messages ATC FANS1/A sont encodés selon une chaîne de caractères hexadécimale respectant le ASN.1 Packed Encoding Rule (INCITS, ANSI) et sont donc plus délicats à décoder. Cependant, des connaissances relativement basiques du système suffisent à la démodulation puis à l'interprétation du paquet.

Une forte communauté de passionnés des communications aéronautiques existe et de nombreux décodeurs sont à disposition afin de permettre l'écoute et le décodage des messages CPDLC (Lemiech, 2017). Il est à la portée de nombreuses personnes de recevoir des messages de contrôle de trafic et la loi autorise leur réception tant que le contenu des communications interceptées n'est pas partagé par la suite (Ministère de la Justice, 1996). Si ces communications appartiennent à "l'espace public" tant qu'elles ne sont pas chiffrées, les compagnies aériennes et les contrôleurs font transiter via la liaison de données des informations qu'ils ne souhaitent pas nécessairement révéler, tel que le démontrent les exemples de messages réels que nous avons nous-mêmes interceptés (Figure 3.1).

```
2017-05-26 17:03:56.044
RX_ID: 307, Freq: 131.550MHz
ACARS mode: 2 (50), label: 4P (Weather report/forecast)
[...]
PNT PA01 Q1A0172 26MAY/1722
X-XXXX/209/0413 XXXXXX/26 YUL YY
GOOD DAY GREG...SUMMER IS COMING UP...
GAS PRICES RISING...
IF YOU'RE INTERESTED IN PICKING UP
SOME DRAFT TOMORROW LET ME KNOW!
GOT A LOV

[2017-05-26 22:32:27.649]
RX_ID: 594, Freq: 131.550MHz
ACARS mode: 2 (50), label: 4R
Block id: 5 (53), msg. no: M95A
Aircraft reg: X-XXXX, flight id: XXXXXX
Type: Boeing 767, carrier: ACA, cn: 33423
Airlines: XXXXX

Message content:-
C3143 HI WE JUST HAD A R ENG HPSOV EICAS MESS.
WITH BLEED LIGHT ON OVERHEAD PANEL. BOTH EXT.
BEFORE WE COULD ACTION THE CHECKLIST.
WE NOW HAVE A R ENG HPSOV STATUS MESS.
```

Figure 3.1 Messages ACARS intercepté à l'aide d'une SDR sur l'aéroport de Montréal Trudeau YUL, le 05 juin 2017

3.1.2 Disponibilité

Faire en sorte que les communications entre les appareils et les centres ATC soient toujours fonctionnelles est l'objectif de *disponibilité*. Si cette dernière était compromise, les conséquences seraient immédiates et relativement importantes pour tout le trafic aérien. Les liaisons de donnée reposent à la fois sur des composantes avioniques et une couche physique radio. Si l'une ou l'autre venait à être indisponible, les communications ne seraient plus possibles via ACARS ou FANS1/A. On considérera dans le cadre de nos recherches que les composantes avioniques des aéronefs sont suffisamment fiables pour mettre de côté l'hypothèse d'une panne, sans compter le fait qu'elles sont souvent redondantes.

Le support physique, lui, est relativement simple à rendre inopérant. Une technique appelée *jamming* consiste à émettre de manière continue sur une fréquence spécifique des données parasites afin de la rendre inutilisable. Les pilotes sont déjà au courant de ce phénomène puisqu'ils font tous face au problème de *stuck mic*, littéralement micro bloqué pendant lequel un appareil émet sans interruption sur les fréquences de contrôle aérien. Heureusement pour la sécurité des vols, les communications ATC sont elles aussi redondantes. Les pilotes disposent de fréquences pour la voix et de liaisons de données en tout temps. Même au-dessus des océans, ils peuvent contacter les contrôleurs compétents via ondes HF ou par satellite si besoin (ICAO, 2013). Bien qu'à l'origine développées en tant que système de redondance, les liaisons de données se sont révélées plus efficaces au-dessus des océans et sont devenues le support de communication primaire. La voix est dorénavant considérée comme le système de secours lors des vols transocéaniques. Une attaque de jamming simultanée sur les fréquences de communication par la voix ainsi que celles dédiées aux liaisons de données reste possible si le pirate possède assez de moyens et est déterminé à rendre toute communication impossible entre un appareil et le sol. Dans ce cas, la seule alternative efficace (à part un changement de fréquence) est de localiser la source des émissions parasites afin de la rendre inopérante.

3.1.3 Intégrité

Assurer l'intégrité des messages de liaison de données consiste à s'assurer qu'au cours de leur vie, les paquets transmis ne sont pas modifiés d'aucune manière. Si l'on veut assurer de manière optimale l'intégrité d'une communication, on doit donc éviter qu'un paquet soit intercepté, modifié puis renvoyé.

Cette notion est relativement proche de celle d'authenticité que nous décrirons par la suite plus en détail et qui est mieux adaptée dans le cas des attaques sur la liaison de données.

3.1.4 Authenticité

Assurer *l'authenticité* des liaisons de donnée dans le cadre de l'ATC consiste à s'assurer que chaque message transmis à un appareil ou à une tour de contrôle provienne d'un utilisateur légitime et soit adressé au bon destinataire.

Il convient également de rendre impossible toute opération de rejeu, c'est-à-dire de capture d'une trame réémise par la suite par un émetteur différent de l'original dans le but de porter préjudice au fonctionnement du réseau. Chaque instruction est toujours envoyée à un avion en particulier (et contiens son immatriculation entre autres informations). Le rejeu d'une commande de contrôle émise pour un aéronef particulier pourrait être reçu par le même appareil au cours d'un autre vol par exemple. Bien que nous n'ayons aujourd'hui aucune preuve d'une attaque par rejeux, des appareils ont déjà reçu des commandes CPDLC destinées à un autre, mais possédant le même indicatif lors d'un vol ultérieur (Selleck, 2017).

Un pilote aurait peu d'intérêt à se faire passer pour un autre appareil puisqu'il est primordial pour lui de recevoir des informations de contrôle pertinentes et lui permettant de progresser en sécurité dans l'espace aérien. En revanche, un pirate pourrait chercher à distribuer de fausses informations sur un aéronef afin de perturber le contrôle de la zone. À l'inverse, usurper l'identité d'un centre de contrôle permet de transmettre aux appareils de fausses indications d'aiguillage.

Le principal danger concernant l'authentification provient donc de potentiels pirates qui enverraient des données volontairement erronées aux appareils en vol ou au sol en se faisant passer pour une entité de contrôle ou un utilisateur aérien légitime. Ce genre d'attaque n'a jamais été réalisée sur les liaisons de données. Néanmoins, l'aéroport de Melbourne a déjà dû faire face à de faux contrôleurs qui envoyaient de mauvaises informations sur une fréquence de communication vocale réservée à l'approche, causant une confusion importante chez les pilotes et contrôleurs concernés (Sveen, 2016).

3.2 Sécurisation des liaisons de données

3.2.1 Rôle des organismes de standardisation

L'existence de failles de sécurité dans les systèmes hautement automatisés et utilisés dans le monde de l'aéronautique semble de plus en plus connue au sein de la communauté scientifique. Des études dressent un portrait alarmant de la situation actuelle dans le transport aérien (Mahmoud et al., 2009) (Teso, 2013). Parmi les systèmes considérés comme vulnérables, on trouve au premier plan les outils de contrôle du trafic aérien (Sampigethaya et al., 2011)

dont font partie les communications par liaison de données. Néanmoins, le développement de moyens de sécurisation efficaces et rétrocompatibles avec des systèmes de plus en plus âgés reste un défi majeur pour de nombreuses raisons.

Le monde de l'aviation repose sur de nombreux mécanismes de régulations et standardisations, longs et exigeants. Cela crée une inertie très forte qui est un frein à l'implémentation rapide de solutions potentiellement efficaces. La taille du parc aéronautique mondial, la complexité des systèmes impliqués et les coûts induits par la sécurité sont autant d'obstacles à la généralisation du recours à des méthodes cryptographiques sur les différents protocoles de communication. La sécurisation des systèmes de communications utilisés dans le milieu du transport aérien ne pourra donc se faire sans l'action sur le long terme de plusieurs acteurs.

L'OACI a identifié depuis quelques années les principaux risques pesant sur les systèmes de communication des avions commerciaux. Selon elle, les usurpations et les modifications liées à l'intégrité et à l'authentification des messages sont les deux attaques les plus préoccupantes (ICAO, 2002). Afin de prévenir ces mêmes attaques, de nombreuses recommandations à l'intention des fabricants de composantes avioniques ont été rédigées au cours des différentes itérations du projet d'ATN (ICAO, 2010). Le document 9880 de l'OACI leur indique le type de solutions à proposer pour obtenir des communications sécurisées au sein de l'ATN, tout en respectant de nombreux critères de performance. Grâce aux alarmes répétées de l'OACI ainsi que de la communauté scientifique internationale, les avions commerciaux de dernière génération sont développés par des équipes ayant conscience des dangers qui pèsent sur les systèmes informatiques en général. Une attention particulière semble donc être accordée à la sécurité des systèmes employés dans les aéronefs les plus modernes comme l'Airbus A350 ou le Boeing 787.

Malheureusement, les compagnies ont généralement à leur disposition des flottes d'appareils qui ont entre 15 et 20 ans (Airsafe, 2016) depuis leur mise en service et encore plus depuis leur développement. Ces avions ont recours de manière extensive à des technologies de communication dont la cybersécurité n'était pas une composante essentielle du design. Aujourd'hui, les seuls consommateurs de communications sécurisées sont les militaires. Ces derniers sont obligés d'être équipés de matériel de communication par liaison de données pour traverser les différentes routes aériennes commerciales (Risley et al., 2001). Pour les appareils militaires, tant la *confidentialité*, la *disponibilité*, l'*intégrité* et l'*authenticité* doivent impérativement être maintenues. Pour répondre à la demande, des solutions sécurisées ont donc été développées par les fabricants d'avionique et ont plus tard mené à des standards tels que ceux développés dans la partie 3.3 ARINC (2016), (Roy, 2001).

Une technologie de communication ne pourra être adoptée massivement que si les compagnies aériennes éprouvent un réel besoin d'équiper les solutions proposées par les équipementiers. La sécurisation de ces mêmes technologies ne peut donc se faire dans les appareils déjà en service sans l'action commune de tous les équipementiers. Cependant, cette dernière ne se fera pas sans un intérêt économique, ou une demande de la part des utilisateurs. Il faudra donc garder à l'esprit que tous les mécanismes décrits dans la partie suivante ne sont que très rarement employés dans les appareils commerciaux. La question des procédés à mettre en place afin de développer leur utilisation est tout aussi cruciale que celle des méthodes de sécurisation elles-mêmes.

3.2.2 Cryptographie symétrique et asymétrique pour les communications aériennes

La plupart des algorithmes récents de cryptographie reposent sur des méthodes dites symétriques, asymétriques, ou encore hybrides en utilisant les deux à la fois. La question de leur utilisation dans le cadre du transport aérien est délicate.

Dans le cas de la cryptographie symétrique, chaque utilisateur nécessite une clé privée partagée avec son interlocuteur. Si tous les couples possibles (avion/contrôleur/opérations) possèdent un unique secret, le nombre de clés privée nécessaires est considérable. Environ 35 000 appareils survolent l'Europe chaque jour environ, soit 612 482 500 couples d'aéronefs potentiels, sans tenir compte des opérations et des centres de contrôle (Eurocontrol). La création ainsi que la distribution sécurisée de toutes ces clés peuvent s'avérer très rapidement complexes. Une solution pourrait consister à partager une clé privée unique au sein d'un même groupe. Si une compagnie souhaite chiffrer toutes les communications entre ses appareils et ses opérations, elle peut renseigner directement au sein de ses appareils le secret partagé nécessaire et l'utiliser sur ses équipements au sol. Néanmoins, l'augmentation du nombre d'acteurs utilisant le même secret accroît d'autant le risque de sa divulgation.

La cryptographie asymétrique permet de passer outre le problème de la distribution des clés grâce au recours à une clé privée, qui reste secrète, et une clé publique, qui peut être distribuée librement. La distribution des clés publiques est confiée à une structure appelée Public Key Infrastructure - PKI. Deux acteurs qui ne se connaissent pas ne devraient pas s'accorder une confiance suffisante afin de mener des opérations normales de contrôle aérien (bien que ce soit aujourd'hui le cas). Ce sont les autorités de certification, ou CA, mises en place par la PKI qui permettent de pallier ce manque de confiance. Une PKI repose sur une hiérarchisation des autorités de certification en haut de laquelle se trouvent des autorités dites *racines*, également appelée *root CA*. Une autorité racine est reconnue par tous les utilisateurs du

système comme étant digne de confiance et n'est certifiée par personne puisqu'elle est située au sommet de la hiérarchie de confiance. Les autorités racines désignent d'autres CA qu'elles considèrent comme fiables et qui certifieront à leur tour d'autres CA. En bout de cette chaîne de confiance, en bas de la hiérarchie, les autorités les plus proches des utilisateurs certifient directement les clés publiques des avions, des centres de contrôle ainsi que des opérations des compagnies aériennes (ARINC, 2008). Tous les acteurs du système accorderont alors leur confiance uniquement si une entité dispose d'un certificat valide associé à sa clé publique.

Bien qu'il permette de passer outre le problème de la distribution des clés, le recours à la cryptographie asymétrique soulève d'autres problématiques. Il nécessite des ressources calculatoires relativement importantes pour la génération des clés. Si nous pensons que l'avionique embarquée dans les avions commerciaux est assez perfectionnée pour permettre la création des paires de clés publique / privée, aucune étude n'a encore définitivement prouvé ce point. En outre, la distribution des certificats et des clés publiques en tant que tels entraîne nécessairement une augmentation de la quantité des échanges sur les réseaux qui peut également poser problème dans un environnement ou la bande passante disponible est limitée.

Une approche hybride pourrait permettre de concilier les avantages des deux méthodes cryptographiques que nous venons de décrire. Néanmoins, les nombreuses problématiques propres aux systèmes de communication par liaison de données sont à prendre en compte.

3.2.3 Problèmes liés à l'utilisation de méthodes cryptographiques

Les solutions cryptographiques mêlant cryptographie asymétrique et symétrique sont depuis longtemps utilisées afin de protéger des systèmes sensibles. C'est par exemple le cas du protocole Secure Sockets Layer - SSL, et de ses différentes itérations, qui permet de sécuriser un grand nombre de communications sur Internet depuis 1995. Malheureusement, les techniques employées par ce protocole ne sont pas nécessairement directement utilisables dans un contexte particulier, comme celui du transport aérien par exemple. Si la cryptographie est un outil évident pour protéger des données numériques, son utilisation dans le contexte des communications par liaison de données est donc loin d'être évidente.

En effet, les algorithmes de cryptographies symétriques sont plus efficaces en termes d'utilisation de la bande passante et de ressources de calcul que les techniques appelées asymétriques.

1. Les techniques de cryptographie induisent la plupart du temps une diminution des performances du système. En effet, le maintien des objectifs de sécurité passe souvent par l'ajout d'informations dédiées supplémentaires. Elles peuvent être ajoutées dans le message lui-même, ou contenues dans des paquets dédiés, lors de l'envoi de certificat

ou de clés par exemple. Une partie de la bande passante disponible devient donc entièrement dédiée à l'utilisation des techniques de cryptographie.

Malheureusement, cette ressource est de plus en plus rare, particulièrement dans le transport aérien puisqu'un nombre croissant d'appareils utilise les fréquences aéronautiques qui doivent être partagées. Ceci force les ingénieurs à considérer à la fois les questions de qualité de service (QoS) et de sécurisation, car elles sont étroitement liées. En effet, la sécurisation des communications par liaison de données grâce au recours à la cryptographie ne peut se faire si le risque de congestion des réseaux dédiés devient trop important, ce qui compromettrait alors la disponibilité des systèmes.

2. Les communications aéronautiques constituent un environnement complexe, car de très nombreux protocoles différents assurent des tâches variées au sein d'un réseau mondial. Les communications au sein d'un appareil reposent sur des standards différents de ceux adoptés pour les communications air-air ou air-sol, etc. Néanmoins, les différents appareils embarqués ou au sol qui permettent les échanges entre acteurs du système doivent toujours être en mesure de communiquer entre eux. L'introduction d'une version sécurisée d'ACARS ne peut se faire que si elle est compatible avec les équipements classiques dédiés à ces échanges. Un paquet, même chiffré, devrait donc être recevable par n'importe quel utilisateur en ayant besoin même s'il n'a pas mis ses propres équipements à jour.
3. Il est très coûteux et délicat de mener une opération de mise à jour des composants avioniques sur un aéronef. Cette dernière nécessite en effet son immobilisation et ne peut se faire qu'après de longs processus de vérification, ce qui engendre des pertes importantes pour la compagnie qui ne peut exploiter son aéronef sur cette durée. Les appareils embarqués suivent donc la plupart du temps l'avion depuis sa conception et la puissance de calcul liée est difficilement améliorable. Si les techniques cryptographiques utilisées par une version sécurisée d'ACARS ou des protocoles FANS1/A comme CPDLC nécessitent une puissance de calcul accrue, il n'est pas certain que l'appareil soit en mesure de la fournir.
4. L'utilisation de méthodes asymétriques implique le recours à une PKI. Pour un système aussi complexe et vaste que celui sur lequel reposent les communications Datalink, il n'est pas évident de déterminer quelle structure sera la plus efficace. Une discussion sur les potentielles formes que pourrait prendre une PKI utilisée par les versions sécurisées d'ACARS est faite en section 3.3.
5. Les solutions disponibles et qui permettent de mettre en place des sessions sécurisées de communication posent des problèmes d'ordre politique. En effet, les standards sont

mis en place par ARINC qui est une compagnie entièrement détenue par Rockwell Collins.

Les systèmes vieillissants offrent la plupart du temps des performances limitées en termes de bande passante. En outre, les protocoles de communication modernes sont la plupart du temps développés afin d'inclure des capacités cryptographiques qui adressent les problèmes les plus urgents mis en avant par l'OACI. Néanmoins, en pratique, des systèmes comme ACARS utilisées depuis plus de 30 ans restent toujours employés, car la majorité des appareils en service sont compatibles.

3.3 Standard AMS - (ARINC 823)

Historiquement, les liaisons de données se sont imposées suite à l'action des avionneurs qui ont développé leurs propres systèmes et les ont mis à disposition des compagnies aériennes. L'US Air Force (USAF) a émis en premier de l'intérêt pour une version sécurisée d'ACARS. La principale préoccupation des avions militaires est de conserver en tout temps la confidentialité des échanges entre les aéronefs et le sol. Afin de permettre ceci, plusieurs équipementiers, dont Honeywell, ont proposé dès 2001 une évolution de la norme ACARS appelée Secure ACARS Messaging - SAM (Roy, 2001). Les travaux sur SAM, une couche applicative assurant la confidentialité d'ACARS, ont par la suite servi de base à la rédaction de la norme ARINC 823 (ARINC, 2007). Ce nouveau type de communication par liaison de données a été nommé ACARS Message Security - AMS. Les couches applicatives SAM et AMS présentent le même type de solutions cryptographiques rétrocompatibles avec les anciens systèmes avioniques. Cependant, SAM est basé sur d'anciennes recommandations de l'OACI (ICAO, 2002) et a recours à des algorithmes maintenant considérés comme faibles et obsolètes tel que SHA1. Ces problèmes ont été adressés dans l'adoption définitive d'AMS.

AMS a été développé comme une couche applicative afin de permettre aux échanges sécurisés et classiques d'ACARS de coexister sur les mêmes réseaux. Ceci permettra également une transition plus facile vers les réseaux ATN quand ces derniers seront définitivement adoptés (Roy, 2001). Ils sont donc totalement indépendants de la couche physique, c'est-à-dire le recours à AMS n'a aucune conséquence sur la forme des paquets envoyés. En revanche, il est nécessaire d'introduire l'utilisation de six nouveaux types de messages qui permettent la mise en place et la terminaison de la session sécurisée. il s'agit de procédures similaires aux *logon* des protocoles les plus récents. Ces nouveaux paquets ACARS sont détaillés à la figure 3.2

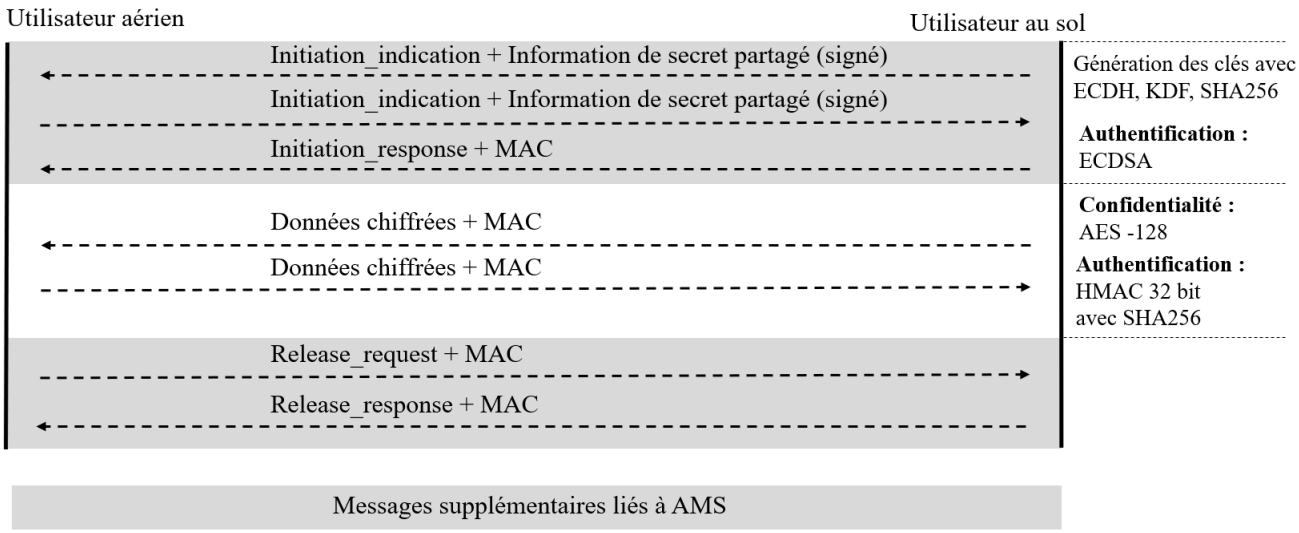


Figure 3.2 Messages dédiés à AMS. Les messages en gris sont introduits par AMS et n'existent pas dans la version classique d'ACARS (ARINC, 2007)

Dans le cas d'AMS, c'est la cryptographie symétrique qui a été choisie comme le principal outil afin d'assurer la confidentialité et l'authenticité du système. Ce choix technique a été fait pour des raisons d'efficacité.

Afin de pouvoir maintenir leurs échanges confidentiels, Alice (l'émetteur) et Bob (le récepteur) partagent une clé secrète K. Ils utiliseront cette même clé pour chiffrer et déchiffrer tous les messages qu'ils sont amenés à s'échanger, via les algorithmes supportés par AMS, tel qu'AES.

Code d'authentification d'un message

En parallèle, le même secret K permet d'assurer l'authentification des messages ACARS, via une technique appelée code d'authentification des messages (ou Message Authentication Code - MAC). Dans SAM, les MAC sont générés de la manière suivante :

— La clé secrète partagée K est calculée par Alice et Bob grâce à un échange d'informations et les deux acteurs la possèdent grâce à un échangé sécurisé.

— Le MAC lui-même est de la forme $\text{MAC} = H(K||M)$ ou $\text{SHA}_{256}()$ représente la fonction de hachage et M représente le message à authentifier.

Chaque fois qu'Alice transmet un message, elle y joindra un MAC. Bob, qui possède également la clé secrète K est capable de le calculer de manière indépendante en utilisant le message qu'Alice lui a transmis. Si les deux sont identiques, il est certain que c'est bien Alice qui

est à l'origine du paquet reçu (le paquet est donc authentifié) et que ce dernier n'a pas été modifié (l'intégrité est alors également vérifiée). En effet, si la clé ou le message ne diffèrent ne serait-ce que d'un seul bit, le haché de la concaténation de la clé et du message, et donc le code d'authentification du message, serait différent.

Malheureusement, ces MAC classiques reposent sur un procédé appelé construction de Merkle-Damgård qui est vulnérable à des attaques dites par *extension* (Bellare et al., 1996). Les fonctions de hachage comme SHA-1 et SHA-2 effectuent les calculs sur des blocs de taille finie (512 bits pour SHA-256 par exemple). Si le dernier bloc a une taille inférieure à 512 bits, il est complété avec des 0. Le haché calculé est donc de la forme $H(K_{MAC}||\mathbf{M}||00...000) = H(K_{MAC}||\mathbf{M}||p)$. Si on applique SHA-256 sur la concaténation de la clé secrète partagée et du message $\mathbf{M}$, elle est découpée en blocs de taille 512 bits et compressée à travers une fonction $f_i = f(f(m_{i-1}, m_{i-2}), m_i)$ dont le premier paramètre est un haché intermédiaire de 256 bits et le deuxième paramètre est le i-ième bloc en cours de traitement. Lors de la première itération $f(V, m_1)$, on utilise un vecteur d'initialisation V.

Il est facile, connaissant la taille de $\mathbf{M}$, de trouver p. En forgeant un paquet de la forme $\mathbf{M'} = (\mathbf{M}||p||z)$ où z est un ensemble de bits arbitraires, on peut anticiper l'état interne de la fonction de hachage lorsqu'elle traitera le début du i-ième bloc (qui correspond à la fin du traitement du message $\mathbf{M}$). Ce processus est explicité dans la figure 3.3. En utilisant cet état intermédiaire comme un vecteur d'initialisation pour la fonction de hachage, on peut calculer le haché valide d'un message contenant des données arbitraires (z) sans connaître la clé secrète K_{MAC} ce qui pose un problème important de sécurité.

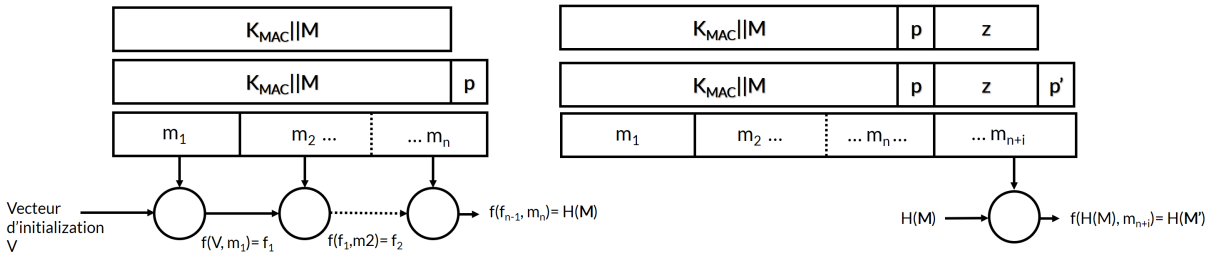


Figure 3.3 Attaque par extension (Bellare et al., 1996)

Afin d'éviter ce type d'attaque, le MAC utilisé par AMS est un keyed-Hash Message Authentication Code (HMAC) (Honeywell, 2009) de la forme :

$$HMAC_{KMAC}(M) = H((K'_{MAC} \oplus opad)\,||H(K'_{MAC} \oplus ipad)\,||\,M)$$

H() est la fonction de hachage SHA-256(), $\oplus$ est l'opération de ou exclusif, et K' représente la clé K_{MAC} que l'on a complétée avec des 0 afin qu'elle ait une taille de 512 bits. Enfin, *opad* et *ipad* sont respectivement les octets 0x36 et 0x5C répétés 512 fois. Le fait d'utiliser un haché intermédiaire à l'intérieur même de la fonction de hachage globale empêche d'effectuer une attaque par extension. En effet, un attaquant n'a de contrôle que sur la taille de l'entrée du haché intermédiaire et non plus du haché "externe" qui prend en paramètre des chaînes de tailles dorénavant fixes, et il lui sera impossible d'insérer des caractères arbitraires.

La norme ARINC-823 part 1 ajoute un HMAC d'une taille minimale de 32 bits aux messages transmis par les utilisateurs du système. Ceci a pour objectif principal de limiter l'augmentation de la taille des paquets, et donc de l'utilisation du réseau, tout en conservant un niveau de sécurité jugé raisonnable. Si besoin, les HMAC peuvent avoir une taille de 64 ou 128 bits.

Plus de 100 000 appareils décollent chaque jour dans le monde et il serait très difficile de distribuer une clé secrète et protéger tous les 4 950 000 000 couples possibles (sans prendre en compte les centres de contrôle, les centres d'opération, etc.). Ceci rend impossible l'utilisation de la cryptographie symétrique seule dans les communications par liaison de données (Mahmoud et al., 2010). Afin de résoudre le problème de la distribution des clés, AMS utilise donc également la cryptographie *asymétrique* dans les handshakes d'initialisation de session.

La cryptographie asymétrique permet de s'affranchir du problème de distribution des clés des algorithmes symétriques via l'utilisation d'une infrastructure à clé publique. La norme ARINC 823 préconise l'utilisation d'une infrastructure à clé publique (PKI) de type UIT X.509, qui est également utilisée afin de sécuriser les sessions SSL/TLS par exemple.

Calcul du secret partagé

Le secret partagé nécessaire aux sessions sécurisées peut être calculé lors de l'établissement de liaison détaille sur la Figure 3.2, grâce à un algorithme appelé Elliptic Curve Diffie Helman (ECDH) (Miller, 1986).

Si Alice et Bob souhaitent établir une session de communication chiffrée, il leur suffit de partager leurs clés publiques K_{pA} et K_{pB}. Alice n'a plus qu'a multiplier la clé publique de Bob par sa clé privée et Bob sa clé privée par la clé publique d'Alice afin d'obtenir une valeur secrète commune. En effet, les valeurs de $K_{pA}K_{sB}$ et de $K_{pB}K_{sA}$ sont les mêmes, car :

$$K_{pA}K_{sB} = (p_A G)p_B = p_A(p_B G) = K_{sA}K_{pB} = Z_{A,B}$$

Cette opération est permise par la commutativité de l'opération de multiplication des courbes elliptiques. On note $Z_{A,B}$ le secret partagé par Alice et Bob.

La clé privée est finalement obtenue en calculant un haché qui nous garantit qu'elle sera toujours de la même taille (Honeywell, 2009) :

$$SHA_{256}(Z_{A,B}||D) = K_{ABsym}$$

Le nonce D contient, entre autres, un chiffre aléatoire connu d'Alice et Bob et $||$ représente la concaténation. D est contenu dans le message *Initiation_Information* transmis par le centre avec lequel on souhaite établir la connexion. Le recours à D nous permet de nous assurer que la clé obtenue sera toujours différente d'une session à l'autre. K_{ABsym} sera utilisée par un algorithme de cryptographie symétrique reconnu comme fiable en l'occurrence AES256.

Signature des paquets sans session sécurisée

L'établissement de liaison permet à tous les acteurs d'obtenir un secret partagé à des fins de protéger la confidentialité de leurs échanges. Ils ne peuvent néanmoins pas encore utiliser la méthode du MAC pour protéger l'intégrité des premiers paquets puisque le MAC repose lui-même sur un secret partagé. Pour palier à ce problème, une signature numérique par courbe elliptique, appelé Elliptic Curve Digital Signature Algorithm (ECSDA) est utilisée dans AMS.

Les signatures numériques permettent à deux utilisateurs, Alice et Bob, qui n'ont pas encore pu calculer de secret partagé d'authentifier leurs premiers échanges sans recours à une clé symétrique. Leur utilisation a été mise en avant par les recommandations de l'OACI (ICAO, 2002), et a donc été adoptée par le standard ARINC 823, qui ajoute à la fin des messages hors session sécurisée (donc sans secret partagé) une signature digitale de 64 octets. La présence de cette signature permet à Bob de confirmer que ce dernier a été émis par Alice et par Alice seulement grâce à la connaissance de sa clé publique.

Gestion des clés cryptographiques

La cryptographie asymétrique, nous l'avons vu, sert de fondation à toute la sécurisation des communications ACARS. Une des conditions nécessaires à l'utilisation d'une telle cryptographie est le recours à une infrastructure à clés publiques ou Public Key Infrastructure (PKI) de type ITU-T X.509 (ARINC, 2008). Grâce à elle, les différentes clés publiques peuvent être distribuées et vérifiées de manière sécurisée.

Si nous avons explicité son fonctionnement, la question des autorités racines utilisables par AMS est relativement complexe à résoudre. Un modèle similaire à ce qui est fait pour Internet pourrait être adopté avec plusieurs CA racines coexistants. Les NAA peuvent apparaître comme de bons candidats. La plupart d'entre elles sont déjà familières avec les mécanismes de certification. Elles possèdent déjà de nombreuses informations sur les appareils qu'elles encadrent ce qui rendrait plus aisé le déploiement d'une PKI dans leur zone d'influence.

S'il est techniquement possible d'étendre cette tâche de certification aux clés publiques utilisée par AMS, ceci n'est pas forcément souhaitable. En effet, parmi les 197 pays reconnus par l'ONU, certains sont instables et soumis à des pressions politiques. Des états peu scrupuleux pourraient être enclins à délivrer de fausses certifications en échange de services financiers, brisant du même coup la confiance accordée dans les certificats autorisés par ce pays et rendant caduque l'utilisation de la cryptographie asymétrique pour certains acteurs. Un moyen de contourner ce problème serait de faire de l'OACI une entité de certification croisée entre les différentes NAA. Elle serait en charge de délivrer des certifications entre les NAA jugées dignes de confiance selon une liste de critères à définir.

Les compagnies aériennes ainsi que les fournisseurs de service Datalink prennent également mesure de la situation et commencent à proposer des solutions. L'état de l'art mené par Mahmoud et al. permet d'identifier les principales architectures en cours de développement (Mahmoud et al., 2014). Tant ARINC que SITA possèdent leurs propres PKI, bien qu'elles ne soient aujourd'hui pas opérationnelles pour l'utilisation qui en serait nécessaire pour AMS. L'Air Transportation Association (ATA), qui rassemble les principaux acteurs américains de l'aéronautique, est à l'origine d'un comité nommé Digital Security Working Group (DSWG). Ce dernier a pu développer des méthodes permettant de lier les infrastructures à clés publiques des principaux acteurs de l'aérospatiale ; elles sont détaillées dans le standard (ATA SPEC 42 : Aviation Industry Standards for Digital Information Security). Le comité inclut des agences gouvernementales comme les NAA, la NASA, l'ESA, etc. Ce processus de coopération est appelé GateLink mais n'est aujourd'hui toujours pas opérationnel.

3.3.1 Travaux de sécurisation de CPDLC

De nombreuses solutions de sécurisation ont déjà été proposées pour ACARS qui est un système relativement ancien. En revanche, il n'existe pas encore de standard de sécurisation pour FANS1/A apparu plus récemment. Néanmoins, plusieurs travaux comme ceux menés par (Rajeswari and Thilagavathi, 2009) proposent d'implémenter des méthodes d'authentification pour CPDLC afin d'éviter les attaques par usurpation. Si les solutions proposées sont très similaires au standard AMS, elles seraient plus facilement implémentables dans les systèmes

avioniques. En effet, dans le cas de CPDLC, il existe déjà des procédures de handshake et de logon lors du premier contact entre un appareil et un centre de contrôle. Il suffirait d'ajouter à ces messages déjà existants les informations nécessaires afin de créer un secret partagé par la méthode décrite dans la partie 3.3.

3.4 Conclusion générale sur la sécurisation de Datalink

Le tableau 3.1 résume les différents travaux de sécurisation qui ont jusqu'à maintenant été mené sur les communications par liaison de données. Les systèmes FANS1/A font référence à l'ensemble des protocoles utilisant le réseau VDL, mais pour lesquels aucun standard de sécurité n'existe encore.

Tableau 3.1 État de la sécurité des communications par liaison de données

	Documentation	Norme	Utilisation
ACARS	Secure ACARS Messaging SAM - 2001	ARINC 823 AMS Part 1&2 -2007/2008	USAF
FANS 1/A	Cryptographie hybride (cf SAM)	Aucune à date	Appareils militaires

SAM, et sa version standardisée AMS, ont été développés pour répondre aux problématiques de sécurité que pose l'utilisation d'ACARS. En conjuguant des techniques de cryptographie symétriques et asymétriques, il est possible de mettre en place des échanges confidentiels tout en garantissant l'authentification des paquets. L'impact sur la bande passante est censé être minimal, mais parmi les nombreuses problématiques que nous avons soulevées en section 3.2.3, certaines restent encore à être adressées dans le cas d'une utilisation civile (rétrocompatibilité des équipements, déploiement d'une PKI adaptée et utilisation d'un standard propriétaire imposant des communications confidentielles). Ces problématiques sont autant de freins à une adoption par l'aéronautique civile d'ARINC 823.

Des solutions similaires à ce que propose AMS seraient adaptées aux protocoles FANS1/A. Néanmoins, malgré les pistes avancées dans la documentation, le déploiement au cours de la prochaine décennie du réseau ATN pose un véritable problème dans la sécurisation de CPDLC. Les communications FANS1/A et le réseau VDLM2 sur lequel elles s'appuient sont relativement récents. De la même manière qu'ACARS over VDLM2 s'est imposé ces dernières années, les protocoles FANS1/A sont jugés assez performants pour être transposées sur ATN. Des versions IP de CPDLC seront donc mises en place et standardisées sous peu (Boeing, 2016). Leur sécurisation est de fait retardée, puisqu'il suffirait d'appliquer les solutions de sécurisation IP qui sont envisagées pour ATN. En l'état, CPDLC resterait donc en service

quelques années, mais n'intégrerait aucune méthode cryptographique avant sa mise en service complète sur les réseaux de nouvelle génération.

Cette situation ne pose en soit pas de problème majeur tant qu'il n'est pas possible d'exploiter une des failles des communications par liaison de données à des fins malveillantes. Nous allons adresser ce point particulier dans la partie suivante.

CHAPITRE 4 ANALYSE DE RISQUE D'UNE ATTAQUE SUR DATALINK

Seuls les avions militaires utilisent de manière intensive les mesures de sécurité qui viennent d'être détaillées. Les appareils civils seraient laissés sans protection de ce genre sur les liaisons de données. La situation déclenche alors une véritable controverse au sein de la communauté scientifique et industrielle sur l'impact réel des vulnérabilités connues dans ces protocoles Datalink. Certains chercheurs prétendent être capables de prendre totalement le contrôle d'un aéronef (Perez, 2015) ce qui contraste fortement avec l'absence apparente de mesure de protection qui n'est justifiée que tant que l'on considère qu'elles ne sont pas nécessaires.

Afin de lever le doute sur la situation réelle, nous allons mener une analyse de risque concernant une attaque sur les liaisons de données. Il s'agit d'un outil pertinent afin d'évaluer avec précisions les dangers qui pèsent sur les communications employées par les avions commerciaux, et offrent entre autres une mesure de l'intérêt de l'investissement dans des solutions comme AMS. Dans un premier temps, les objectifs de sécurité exploitables par un attaquant doivent être identifiés.

4.1 Méthodologie de l'analyse de risque

Il n'est pas évident de déterminer les attaques qui causeraient le plus de dégâts sur les communications par liaisons de données des avions commerciaux. Une approche répandue consiste à dégager des acteurs de menace ainsi que vulnérabilisés qu'ils pourraient exploiter des failles dans des scénarios d'attaque précis (Stallings and Brown, 2014). Une fois ces différents éléments mis en évidence, pour chaque combinaison possible d'attaquant et de scénario on tente de déterminer quelle est la *probabilité* de réalisation de l'attaque. La probabilité employée ici n'est pas une probabilité au sens mathématique strict du terme. Elle est définie comme étant l'agrégation des coefficients affectés à trois caractéristiques :

- La *capacité* C quantifie la facilité avec laquelle un acteur peut avoir accès aux ressources (aussi bien intellectuelles que matérielles) qu'il est nécessaire de posséder afin de mener avec succès une attaque.
- La *motivation* M représente l'intérêt qu'aurait un agent de menace à compromettre le système que nous cherchons à défendre. Elle est entre autres déterminée en fonction de ce qu'aurait à gagner un acteur si un scénario d'attaque se déroule avec succès.
- Enfin, *l'opportunité* O permet de jauger la facilité avec laquelle il est possible d'accéder à un moyen de compromettre ce même système (physiquement ou non) à la fois dans

le temps et dans l'espace. Il peut s'agir par exemple d'un accès au cockpit, au système WiFi de l'avion, aux communications longue distance, etc.

Couplé à la probabilité, l'indice d'*impact* I permet de conclure notre analyse de risque. Ce dernier représente les dommages causés au fonctionnement du contrôle du trafic aérien si une attaque portait sur la caractéristique associée de la liaison de données. L'impact peut être de plusieurs natures. Il peut d'une perte monétaire liée à un délai dans les opérations de vol, à un accident suite à la perte de passagers ou enfin à une perte de la réputation si le public n'est plus en mesure d'accorder sa confiance en une compagnie.

On suit donc la démarche suivante :

- $P = C + M + O$
- Espérence E = Probabilité $*$ Impact $= P * I$
- On traite les objectifs de sécurité pour lesquels E est le plus élevé.

4.1.1 Classification des objectifs de sécurité

Les communications via liaisons de données sont nécessaires au bon déroulement des vols. En cas d'attaque, chacun des objectifs de sécurité que nous avons déjà décrits est concerné. Néanmoins, il n'est pas nécessairement pertinent d'analyser toutes les failles en termes de confidentialité, de disponibilité, d'intégrité ou d'authentification.

En effet, il est plus difficile de réaliser une attaque qui affecte certains objectifs de sécurité que d'autres. Autrement dit, rendre indisponible une fréquence radio en la brouillant (ce qui concerne la disponibilité du système) nécessite beaucoup plus de moyens que d'intercepter des communications non chiffrées afin d'obtenir des informations potentiellement sensibles transmises par un appareil en vol (à cause d'un manque de confidentialité). La capacité de l'attaquant varie donc grandement selon l'objectif considéré. Nous nous contenterons donc par la suite de décrire des scénarios qui peuvent être facilement réalisés, car ils nécessitent des capacités matérielles et intellectuelles relativement faibles, ce qui augmente le nombre d'attaquants potentiels *in fine*.

Le tableau 4.5 permet de quantifier l'impact de l'attaque d'un acteur externe qui chercherait à compromettre l'un ou l'autre des objectifs de sécurité de notre système. L'échelle de cotation du tableau 4.4 aurait pu être différente, mais permet de définir une référence pour comparer les différentes menaces les unes aux autres. Les indices des différentes caractéristiques de sécurités se basent sur nos propres estimations suite à des échanges informels avec des pilotes de ligne aériennes avec qui nous avons eu l'occasion de discuter à trois reprises, ainsi qu'après analyse des recommandations de l'OACI (ICAO, 2002).

Tableau 4.1 Échelle de cotation d'impact

Côte	Classification [1]	Description
1	Mineur (NON CRITIQUE)	petite perte monétaire, presque Aucun impact sur le fonctionnement normal des opérations, etc.
2	moyen (CRITIQUE)	Perte monétaire moyenne, perturbation du trafic Peu dommageable, blessures légères à moyennes.
3	majeur (TRÈS CRITIQUE)	Perte monétaire liée à un arrêt des opérations de plusieurs heures, modifications importantes de la trajectoire d'un appareil, déclenchement alerte TCAS, blessures moyennes à majeures, bris d'équipements, etc.
4	Catastrophique (VITALE ; «MISSION CRITICAL»)	Arrêt indéfini, perte de millions de dollars, perte ou crash d'un appareil, blessures graves à très graves, perte de vie, etc.

Tableau 4.2 Échelle de cotation de Capacité

Côte	Classification	Description
1	Capacité faible	Les ressources matérielles et intellectuelles nécessaires à l'exploitation de cette faille sont très exigeantes et très peu d'acteurs sont en moyen de les collecter.
2	Capacité modérée	Les ressources matérielles et intellectuelles nécessaires à l'exploitation de cette faille sont disponibles, mais nécessitent des moyens importants.
3	Capacité élevée	Il est possible de réunir la plupart des ressources matérielles et intellectuelles nécessaires à l'exploitation de cette faille.
4	Capacité très importante	Il est très aisé de réunir toutes les ressources matérielles et intellectuelles nécessaires à l'exploitation de cette faille.

La confidentialité des messages échangés par liaison de données, même si elle n'est pas garantie, ne remet pas en question la sécurité du vol directement. Les agents impactés les plus directement sont les passagers et les pilotes qui risquent de voir des informations personnelles révélées (comme des numéros de carte de crédit lors des transactions au cours du vol qui sont parfois effectuées via Datalink ou des conversations privées). Assurer la confidentialité des échanges entre les aéronefs et les contrôleurs ne sera donc pas un objectif de sécurité primor-

Tableau 4.3 Échelle de cotation d'opportunité

Côte	Classification	Description
1	Faible	Il y a peu de chances de pouvoir exploiter cette faille.
2	Modérée	Un acteur peut avoir des occasions d'exploiter cette faille.
3	Élevée	Un acteur a de fortes chances de pouvoir exploiter cette faille.
4	Opportunité très élevée	S'il le souhaite, un acteur exploitera cette faille.

Tableau 4.4 Échelle de cotation de motivation

Côte	Classification	Description
1	Motivation faible	Un acteur de menace n'a que très peu d'intérêt à exploiter cette faille.
2	Motivation modérée	Un acteur de menace peut avoir des raisons à exploiter cette faille.
3	Motivation élevée	Un acteur de menace cherchera à exploiter cette faille.
4	Motivation très élevée	Un acteur de menace fera tout ce qui est en son pouvoir pour exploiter cette faille.

Tableau 4.5 Analyse des facteurs de probabilité sur les communications par Datalink (acteurs externes)

	Capacité	Opportunité	Motivation	Probabilité	Impact	Risque
Confidentialité	4	3	3	10	1	10
Disponibilité	2	2	3	7	4	28
Intégrité	4	3	2	9	3	27
Authentification	4	3	3	10	4	40

dial, car l'impact induit par la compréhension de messages par des acteurs non désirés est minime.

Les deux caractéristiques à protéger en priorité des communications par liaison de données sont leur disponibilité et leur authenticité puisque ce sont les deux pour lesquels le risque est le plus élevé. Le système doit en effet toujours être à disposition des pilotes et des contrôleurs aériens, sans quoi le contrôle du trafic serait grandement ralenti lors des traversées transocéaniques. En outre, certains cas de personnes se faisant passer pour des contrôleurs aériens ont déjà causé des perturbations dans certains aéroports (Sveen, 2016), prouvant l'importance capitale de l'authentification des paquets. Du matériel bon marché et facilement accessible permet de faire l'émission de paquets ACARS ou CPDLC, là où il est plus coûteux de brouiller

une fréquence radio afin de la rendre indisponible. En outre, les systèmes de contrôle sont redondants (Strohmeier et al., 2017). Rendre indisponible de manière efficace un certain type de communication nécessiterait donc de s'attaquer à deux systèmes de manière simultanée. De cette analyse découle que :

Les attaques les plus préoccupantes sont les attaques qui exploitent le manque d'authentification des messages de liaison de données.

Ces résultats sont en accord avec les recommandations avancées par l'OACI envers les attaques d'usurpation qui exploitent les lacunes en termes d'authentification. En effet, les codes inclus dans les trames et utilisés afin d'adresser un message à un appareil ou à un centre de contrôle en particulier sont aisément falsifiables. Encore aujourd'hui, aucun mécanisme cryptographique permettant de contrôler l'authenticité d'un paquet ACARS ou FANS1/A n'a été mis en place à grande échelle.

4.1.2 Agents de menace

Il est difficile et peu pertinent de tenter de distinguer précisément quels sont les potentiels attaquants de notre système. Si certaines pistes peuvent être considérées grâce à des études cherchant à obtenir une liste précise des acteurs qui risqueraient de lancer une cyberattaque sur les transports aériens (Arasly, 2005), (Lam et al., 2017). Les résultats obtenus ne permettent malheureusement pas de distinguer de manière exhaustive les éventuels agents de menace, même si certaines pistes sont exploitées. Ainsi, les scénarios d'attaque que nous détaillons par la suite impliquent une première action de la part d'acteurs extérieurs tels que des groupuscules terroristes ou des états voyous.

Une fois de plus, nous ne tenterons pas d'établir une liste précise des personnes à même de mener une attaque contre les systèmes de communication des avions commerciaux puisque nous estimons que cette question est en dehors du périmètre de nos recherches.

En revanche, il est possible de faire une séparation claire entre les acteurs internes et externes au système. Les pilotes, les contrôleurs aériens et les opérations de compagnies aériennes ont un accès direct aux communications par liaison de données puisqu'ils en sont les utilisateurs légitimes. Ces derniers possèdent tous les connaissances et moyens techniques pour provoquer de sérieuses perturbations du trafic aérien. Néanmoins, nous choisissons de ne pas traiter les scénarios d'attaques qui seraient exclusivement menées par des acteurs internes. Nous estimons que les accidents impliquant des actes volontaires comme celui du vol 9525 de la Germanwings, perdu suite à un acte délibéré du copilote de l'appareil (BEA, 2016), sont hors sujet de notre étude.

4.2 Scénarios d'attaque

S'il n'est pas exploitable à des fins malicieuses, le manque d'authentification des communications par liaison de données ne serait pas un problème. En revanche, s'il s'agit d'un élément qu'un attaquant peut exploiter afin de mettre en péril le fonctionnement normal d'un ou plusieurs vols, il devient important d'adresser cette lacune. Toutes les informations présentées dans la suite de cette partie ont été obtenues au cours d'entretiens avec du personnel navigant canadien. Nous avons entre autres demandé à des pilotes de confirmer pour les deux systèmes de liaison de données les plus utilisés aujourd'hui (ACARS et VDL-FANS1/A) des scénarios crédibles d'attaques que nous avons nous-mêmes imaginés. Il est à noter qu'il existe probablement d'autres moyens de compromettre la sécurité des vols en utilisant la liaison de données, mais que les méthodes décrites permettent déjà de sérieusement compromettre les opérations aériennes classiques.

4.2.1 ACARS

Les possibles utilisations des liaisons ACARS ont déjà été détaillées dans le tableau 1.1. Bien qu'ils permettent encore de nombreuses choses, les messages ACARS sont principalement utilisés pour les échanges AOC, c'est-à-dire les communications entre les pilotes et les compagnies aériennes (les *opérations*). Certaines compagnies comme Air Canada possèdent même leurs propres fréquences VHF exclusivement dédiées à l'AOC (131.475 MHz) (ARINC, 2007). Les messages de la figure 4.1 ont été interceptés à l'aéroport de Montréal Trudeau à l'aide d'une SDR et d'un ordinateur grâce au procédé qui a déjà été explicité dans le Chapitre 3.

```
Message content:-
.PERFFQK 301725
AGM
AN IMAT/FI FLIGHT NUMBER
-  AERODATA PERFORMANCE UPLINK
-----------
TAKEOFF DATA FLIGHT :8030   REL  1
MAY 30 2017 17:25:43Z
WIND      170/14
TEMP      P15
QNH       30.00
GTOW      45567
INDEX
   -----
REMARKS   WET RUNWAY
          WB DATA MISSING
-----------
YUL 24L                 9600 FT
DT H237                 FLAP  8
FRA       1118         V1   137
FULL - RLNG - BL OPEN  VR   137

N1      90.2   AT/---  V2   147
MAXN1     92.3        VT   175
MTOW      50143/A
-----------
171 PROCESSED
```

Figure 4.1 Messages ACARS AOC lors du calcul des vitesses pour le décollage

La séquence de trois messages présentée sur la figure 4.1 a particulièrement retenu l'attention des pilotes auxquels nous avons présenté nos travaux, car ils permettent de causer d'importantes perturbations lors du décollage d'appareils (pour des raisons de sécurité, les informations concernant l'appareil et la compagnie ont été masquées).

Lors de la préparation d'un vol commercial, l'équipage doit prendre en compte de nombreux paramètres comme la masse de l'appareil, ses performances, la longueur de la piste disponible et son état, afin de calculer les vitesses optimales pour le décollage. On obtient alors trois "V speeds" appelés V_1, V_r et V_2.

Selon les définitions de Transport Canada (Transport Canada, 2016) :

— V_1 désigne la "vitesse de détection de panne de moteur critique" à partir de laquelle il n'est plus possible d'annuler le décollage de l'appareil quoiqu'il arrive. En effet, une fois que l'aéronef a atteint V_1, il ne reste plus assez de piste disponible pour permettre d'avorter la procédure de décollage en sécurité.
— La vitesse V_r désigne la "vitesse de rotation" à laquelle le pilote doit lever le nez de son appareil. Elle est telle que la portance qui s'applique sur les ailes de l'avion est suffisamment importante pour lui permettre de quitter le sol quelques secondes après que le pilote ait tiré le manche.
— Enfin, V_2 représente la "vitesse de sécurité au décollage". En d'autres termes, il s'agit de la vitesse à adopter afin de commencer la montée de l'aéronef. Toutes ces données sont résumées dans la figure 4.2.

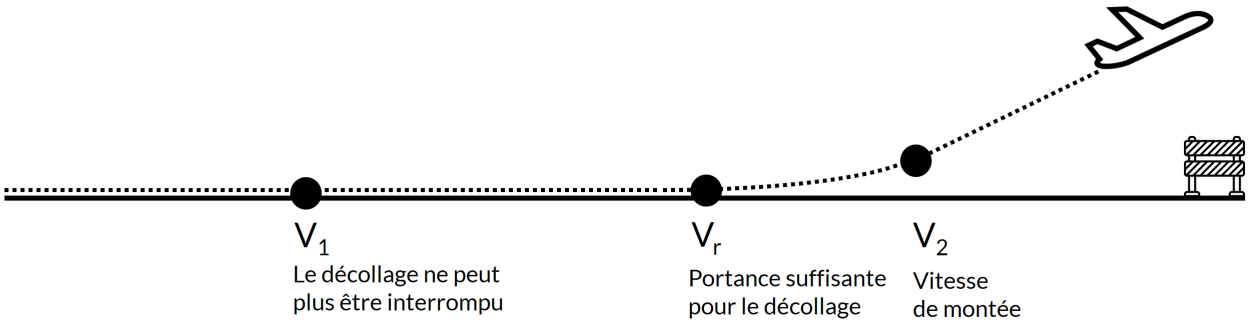


Figure 4.2 Vitesses V au décollage d'un appareil

Il n'est pas possible de donner les fonctions mathématiques précises utilisées pour le calcul de ces vitesses puisqu'elles dépendent grandement des performances de chaque appareil ainsi que des règles internes aux compagnies aériennes.

Quelle que soit la compagnie, une partie des informations nécessaires au calcul de V_1, V_2 et V_r qui dépendent de facteurs comme la météo, l'état des pistes en service, etc. sont obtenus grâce à l'*Automatic Terminal Information Service* - ATIS. Il s'agit d'un service de radio fourni par les aéroports permettant de transmettre aux appareils toutes ces informations. Les données peuvent être envoyées par un message vocal enregistré ou via ACARS (il s'agit dans ce cas du Digital-ATIS). Les pilotes contactent aussi éventuellement les opérations de la compagnie en charge du vol afin d'obtenir les données sur les passagers et le chargement de l'avion.

Une fois toutes les informations nécessaires réunies, l'équipage suit une procédure définie par la compagnie pour laquelle il effectue le vol. Certaines fournissent par exemple à leurs personnels navigants des tablettes pourvues d'applications dédiées sur lesquelles il est possible

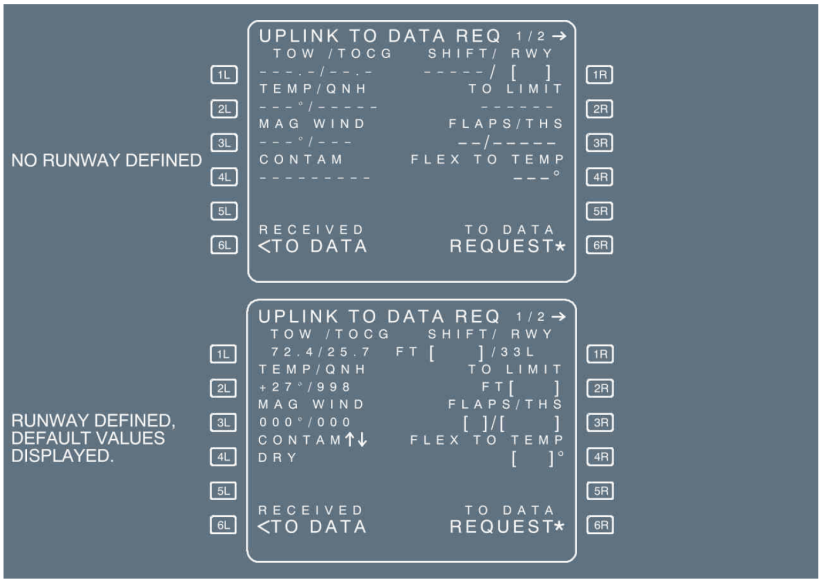
d'entrer les données de masse et météorologiques. Les différentes vitesses à adopter au décollage sont donc calculées au sein du cockpit et le personnel navigant n'a plus qu'à introduire manuellement dans le système de gestion de vol, ou *Flight Management System*- FMS, les informations fournies par la tablette. Il existe d'autres méthodes qui permettent aux pilotes de calculer les V_1, V_2, V_r de leur appareil au début de chaque vol qui se reposent sur un calcul à l'intérieur même du cockpit. Elles peuvent être considérées comme sécuritaires vis-à-vis d'une attaque sur les communications tant que les données ATIS sont valides.

D'autres compagnies aériennes préfèrent effectuer le calcul des vitesses et puissance moteur au décollage directement sur des serveurs privés dédiés au sol. Une fois que le pilote a reçu les données sur l'appareil (chargement, nombre et poids des passagers, etc.), il envoie via ACARS un message comportant les informations ATIS ainsi qu'un résumé des conditions de centrage de l'avion aux opérations. Le serveur étant capable de communiquer via ACARS, il lui transmet en retour les vitesses et puissances de décollage, qui sont imprimées et rentrées dans le FMS, ou rentrées automatiquement si le pilote les accepte et si l'appareil le permet. C'est précisément le même type de message que présente la figure 4.1, qui a été intercepté à l'aéroport de Montréal Trudeau.

L'augmentation de l'automatisation facilite grandement les attaques. En effet, si elle ne supprime aucunement la responsabilité du pilote vis-à-vis de la vérification dans le processus de calcul des vitesses de décollage, elle peut mener certains équipages à lui accorder une confiance élevée. Un pilote pourrait être tenté de ne pas systématiquement vérifier les informations que lui indique son avionique, ce qui nous a été confirmé lors de nos entretiens avec des personnels navigants. En effet, les différents équipages que nous avons contactés nous ont affirmé qu'ils ne vérifiaient pas souvent les vitesses V reçues des opérations et ont toutes les chances de rentrer de fausses données tant qu'elles sont reçues via la liaison de données. Un exemple de ce type de système automatisé pour le FMS de l'Airbus A320 est donné sur la Figure 4.3.

En suivant une procédure comme montrée sur la figure 4.4, un pirate pourrait donc introduire des informations erronées sur un appareil au cours du processus d'échange de données.

À aucun moment un contrôle des séquences des messages envoyés n'est effectué, ce qui peut laisser une grande marge de manœuvre aux attaquants qui n'ont pas besoin d'être authentifiés, car ce système utilise ACARS. Si un seul des paramètres nécessaires au calcul de V_1, V_2 et V_r venait à être modifié, les vitesses finales se retrouveraient erronées. Falsifier les messages en provenance d'un avion sur le point de décoller, des opérations ou bien même de l'ATIS pourrait donc suffire à mettre en péril le décollage.



TITLE	White.
[1L] TOW/TOCG (green)	This field is dashed, until a runway is defined in the [1R] field. The TOW/TOCG is defaulted to the values of the INIT B and FUEL PRED pages. If not available, dashes are displayed. It cannot be modified by the pilot.
[2L] TEMP/QNH or QFE (green/blue)	This field is dashed, until a runway is defined in the [1R] field; TEMP = Defaulted to SAT, and cannot be modified by the crew. BARO = Defaulted to FCU selection and can be modified by the pilot.
[3L] MAG WIND (blue)	This field is dashed, until a runway is defined in the [1R] field. It displays the wind at the origin. The pilot can modify this field.
[4L] CONTAM (blue)	This field is dashed, until a runway is defined in the [1R] field. The display is defaulted to DRY. The scroll keys are used to modify the runway contamination: DRY, WET, 1/4 WATER, 1/2 WATER, 1/4 SLUSH, 1/2 SLUSH, COMP SNOW.

Figure 4.3 Flight Crew Operating Manual - FCOM Airbus 318/319/320/321. On observe sur le FMS du bas une requête uplink via liaison de données de la part des opérations au sol afin d'indiquer à l'équipage quelles sont les conditions pour le décollage (piste sèche, vent, piste à emprunter, etc.). Le pilote n'a plus qu'à les accepter afin qu'elles soient prises en compte par l'avionique de son appareil (Airbus Training and Flight Operations Support and Services, 2005).

Revoir la charge totale à la baisse, augmenter la vitesse des vents, mal juger l'état de la piste est autant de modifications qui entraîneraient potentiellement une diminution des vitesses de décollage. Un pilote habitué à des procédures strictes ne chercherait plus à abandonner le décollage dès lors qu'il pense avoir dépassé V_1. Au moment de tirer le manche, la portance sur les ailes ne serait cependant pas suffisante pour permettre à l'appareil de quitter le sol.

Cette situation peut aboutir à des accidents appelés *tailstrike*, c'est-à-dire une rotation sans décollage de l'appareil pouvant mener à un contact de la queue de l'avion avec la piste. En plus des dommages potentiellement causés par le choc, le pilote n'a plus que quelques secondes pour mettre les pleins gaz ou risque de mener l'appareil à une course jusqu'en bout de piste. Lors du vol de la compagnie Emirates EK407 du 20 mars 2009 (ATSB, 2009), l'équipage, distrait, a entré dans son FMS de mauvaises informations concernant la masse de l'appareil, ce qui a entraîné entre autres un mauvais calcul de V_1 et V_r. Au moment de la rotation, la vitesse étant insuffisante l'appareil n'a pas quitté le sol bien qu'il ait cabré, et a fini par heurter le seuil de piste tout en causant des dommages sévères à sa queue ainsi qu'au fuselage. Bien qu'il ai fini par décoller en détruisant les lumières en seuil de piste, l'appareil a été contrait de faire demi-tour et de se poser en urgence à l'aéroport de Melbourne après que de la fumée ait rempli l'habitacle. Aucun passager n'a été blessé, mais l'Airbus A340 a dû être mis hors service pendant plusieurs mois pour des réparations, et a causé d'importants retards et des pertes financières élevées à son opérateur.

Cet exemple prouve que les pilotes ne sont pas toujours très vigilants sur l'exactitude de ces vitesses. En composition avec notre attaque permettant d'introduire des erreurs délibérées dans ce processus, un incident à gravité similaire pourrait avoir lieu.

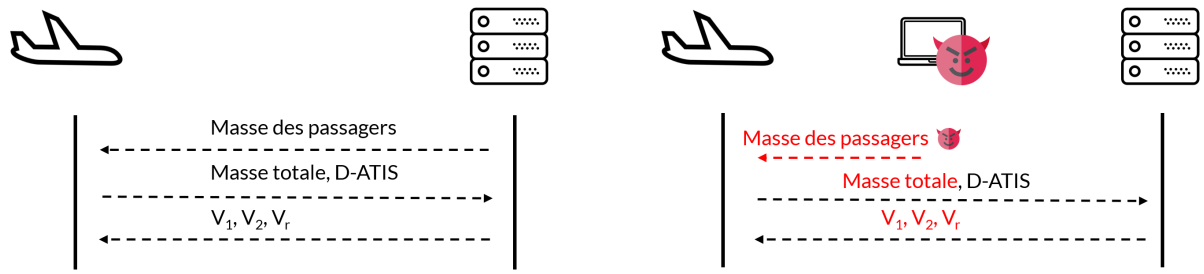


Figure 4.4 Scénario d'attaque sur ACARS

Cette attaque est n'est pas la seule qu'il est possible de réaliser via l'envoi de faux paquets ACARS. Néanmoins, il s'agit incontestablement de la plus aisée à réaliser, car les appareils sont encore au sol, et donc faciles d'accès, car une faible puissance d'émission suffit à atteindre

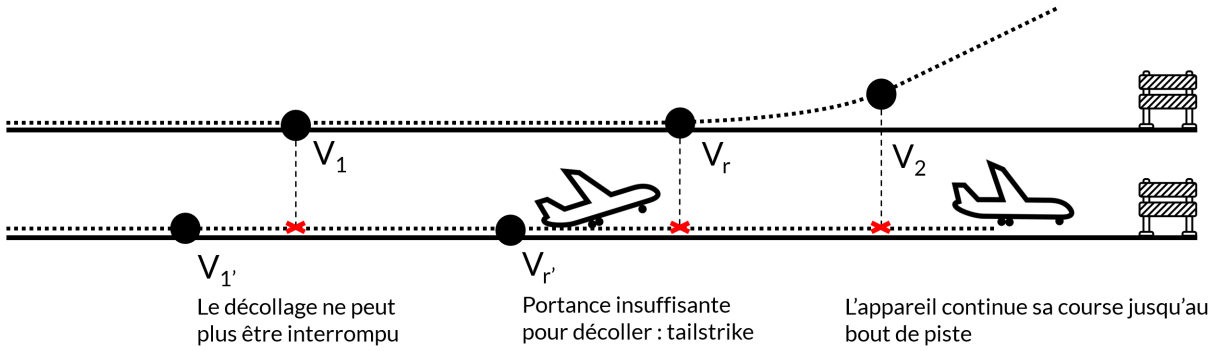


Figure 4.5 Exemple de tailstrike induit par de fausses vitesses V (ATSB, 2009)

les avions sur le point de décoller ce qui augmente le facteur d'opportunité pour un éventuel attaquant.

4.2.2 CPDLC

Nous l'avons vu, même si elles sont encore utilisées pour le contrôle du trafic aérien, dans le cas précis des échanges avec les centres de contrôle, les liaisons ACARS ont en partie été remplacées par les protocoles FANS1/A comme CPDLC et ACARS sur VDL, spécialement développée pour cet usage.

La majeure partie du parc aérien est équipée de moyens de communications de liaison de données car ces derniers facilitent grandement les opérations de contrôle et sont en place depuis plusieurs années. En outre, l'OACI pousse encore aujourd'hui les appareils commerciaux à utiliser les liaisons VDL dans le cadre de son plan de déploiement de l'ATN (UASC, 2017).

En revanche, les centres de contrôle ne se basent pas tous sur la même technologie afin de contacter les appareils. Cela est principalement dû aux actions des NAA qui optent pour des choix différents lors du déploiement des réseaux Datalink. NAV Canada et la DGAC, par exemple, ont adopté des stratégies très différentes lors de la mise en place de VDLM2. Les dernières informations publiques communiquées par la SITA en 2009 font ainsi la démonstration de la disparité entre l'Europe (qui utilise le VDLM2 de manière intense) et les États-Unis (qui ont historiquement préféré se baser sur ACARS). Ces différences dans le déploiement des réseaux Datalink de nouvelle génération sont montrées sur la figure 4.6 (SITA, 2016).

Un scénario d'attaque sur CPDLC est relativement simple à imaginer. En effet, au-dessus des océans, la majorité des ordres de contrôle transitent directement via FANS1/a et il suffit de

disposer de matériel adapté pour qu'un attaquant puisse usurper l'identité d'un contrôleur aérien (avec toutes les implications imaginables).

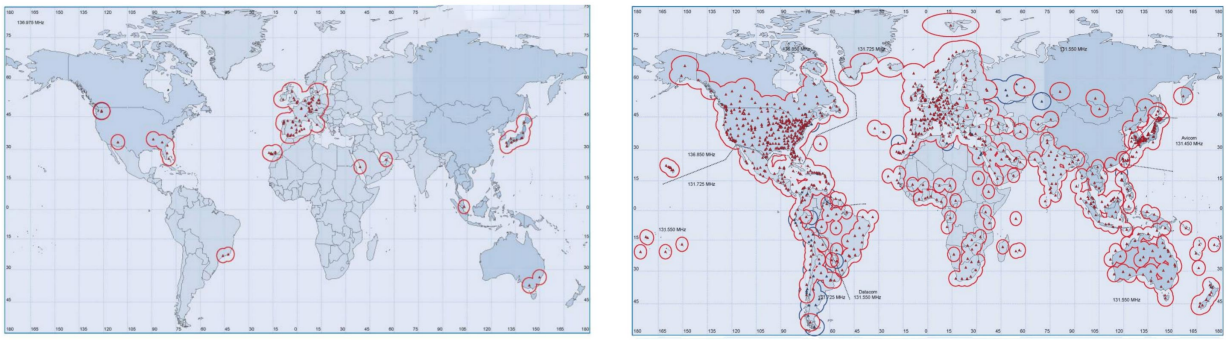


Figure 4.6 De gauche à droite : Réseau VDLM2, Réseau ACARS VHF SITA (SITA, 2016)

La grande variété de l'équipement de communication utilisé se traduit directement dans les procédures suivies par les pilotes lors de traversées transatlantiques entre l'Europe et le Canada. Le centre de Gander au Labrador, responsable des côtes canadiennes et du secteur nord Est de l'Atlantique Nord, transmet ainsi aux équipages les autorisations océaniques - OCL via le protocole ACARS. A contrario, le centre de Shanwick [2], communique toutes les informations utiles aux pilotes, c'est-à-dire les autorisations océaniques ainsi que les ordres ATC, par CPDLC, puisque le réseau VDLM2 a été déployé plus rapidement en Europe. Tant qu'ils évoluent dans la zone de contrôle couverte par Shanwick, les appareils reçoivent donc la majorité de leurs instructions par liaison de données, comme ACARS sur VDL ou CPDLC. C'est ici que les avions seront les plus vulnérables à une quelconque attaque sur les systèmes de communication CPDLC.

Les entretiens que nous avons pu mener avec différents pilotes de nous ont toujours permis de tirer la même conclusion. Une instruction reçue par CPDLC, tant qu'elle ne paraît pas contraire au sens commun, sera suivie pour deux raisons.

Premièrement, les procédures classiques d'échange entre un centre de contrôle et un appareil en vol autorisent plusieurs types de messages comme détaillés dans le document GOLD, qui définit les règles d'utilisation de CPDLC (ICAO, 2013). Un centre de contrôle peut demander l'avis d'un équipage sous la forme de messages interrogatifs, ce qui laisse une certaine marge de manœuvre pour accepter, ou non, une autorisation ou un ordre de modification de trajectoire. En revanche, il n'y a, a priori, aucune raison de remettre en question un message impératif de type "DESCEND AT * MAXIMUM RATE".

2. Issu de la fusion des centres de Shannon en Irlande et Prestwick en Écosse

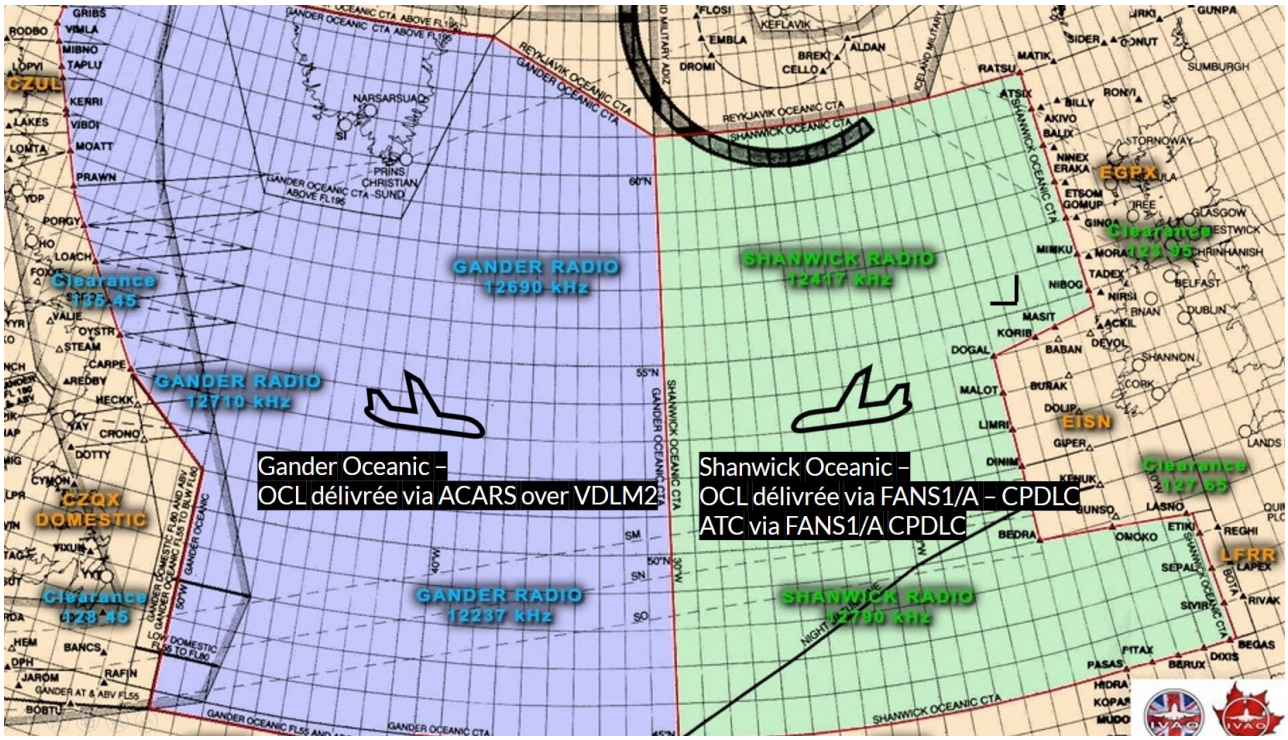


Figure 4.7 Zones de contrôle du trafic aérien au-dessus de l'Atlantique

En outre, la plupart des pilotes ne remettent pas en question le bien fondé ni l'origine des messages reçus par liaison de données. Plusieurs études menées à grande échelle sur les professionnels du transport aérien avancent que seuls 10% des équipages estiment que le CPDLC ne garantit pas l'authenticité des informations transmises, comme montré sur la figure 4.8 (Strohmeier et al., 2017). Ce sentiment est d'autant plus fort qu'il est bien plus difficile de différencier un contrôleur professionnel d'un attaquant sans recours à la voix.

Des notes de sécurité ont été émises dans de nombreux aéroports afin d'interdire provisoirement le recours aux communications CPDLC durant l'année 2017 (Selleck, 2017). En effet, plusieurs appareils ont suivi des ordres qui ne leur étaient pas destinés, mais qu'ils ont reçus de manière accidentelle (Trautvetter, 2017) suite à des problèmes techniques. S'ils ont été rapidement détectés et ont eu des conséquences minimes, ces incidents démontrent qu'une simple attaque par rejeu aurait de grandes chances de fonctionner. Un minimum de connaissances informatiques suffit à capturer des paquets puis à les rejouer. De telles manœuvres sont réalisables à l'aide de matériel peu dispendieux. Il devient donc primordial de prévenir l'action d'un pirate déterminé aux connaissances techniques suffisantes.

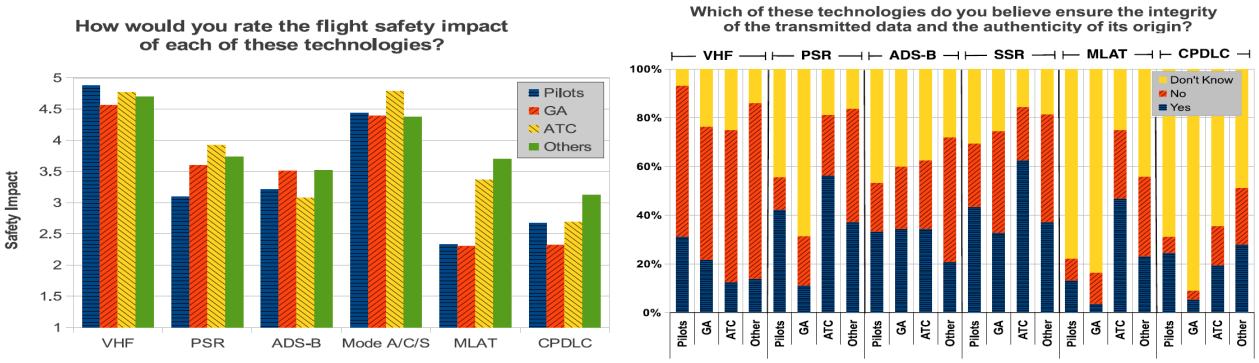


Figure 4.8 Évaluation des technologies ATC, impact sur la sûreté et la sécurité (authentification et intégrité). Ces données ont été obtenues suite à des échanges avec 43 pilotes de ligne, 55 pilotes privés, 32 contrôleurs et 45 autres personnes. Elles montrent le degré de confiance que les équipages accordent dans leurs systèmes de communication (Strohmeier et al., 2017).

Si un attaquant décidait de créer lui-même des paquets CPDLC, il serait en puissance capable de modifier suffisamment la trajectoire d'un avion afin de créer une situation de conflit de séparation, de déclenchement d'alarme anticollision et voir même dans des circonstances extrêmes de collision, puisque l'équipage exécuterait toutes ses demandes tant qu'elles paraîtraient suffisamment crédibles. Ceci ne serait évidemment possible que si de nombreux facteurs sont réunis en même temps.

Si plusieurs informations peuvent encore permettre à un pilote de réaliser qu'il suit de fausses instructions, comme un visuel sur un autre appareil ou le systèmes d'évitement de collision *Traffic Collision Avoidance System* - TCAS actifs par exemple, d'éventuels pirates peuvent néanmoins avoir une influence sur une des sources d'information du personnel navigant. En outre, les communications aéronautiques sont hautement procédurales et tout centre de contrôle constatant qu'un appareil dévie de sa trajectoire nominale chercherait à entrer en contact avec lui. Une attaque échouerait donc tant que les procédures déjà mises en place permettent de détecter et corriger une anomalie plus rapidement que le temps nécessaire à deux avions proches pour rentrer en conflit de séparation.

4.2.3 Considérations sur l'impact des scénarios d'attaque

Nous n'avons proposé deux scénarios exploitant le manque d'authentification d'ACARS et de FANS1/A. À notre surprise, l'analyse de quelques paquets ainsi que de brèves discussions avec des pilotes de ligne nous ont suffit à trouver des situations dangereuses pour les appareils commerciaux. À aucun moment nous n'avons engagé des connaissances pointues des

procédures aéronautiques. Une simple curiosité du sujet ainsi que des recherches méticuleuses nous ont permis de développer des situations plus que plausibles d'attaque potentiellement sur les communications par liaison de donnée. Ces deux scénarios dépendant de nombreux facteurs qui doivent tous concorder afin de mener à la réussite d'une attaque. Dans le premier cas, la compagnie visée doit par exemple calculer ses vitesses au décollage sur un serveur qui communique par ACARS. Il faut également réussir à injecter des informations erronées au moment opportun, et compter sur un manque de vigilance du pilote lors de la validation des informations reçues.

Nous pensons néanmoins qu'il est possible, si ce n'est facile, d'envisager des situations ou tous ces éléments concordent afin de permettre une attaque. Si cela ne conduit pas nécessairement à un écrasement ou la perte de contrôle totale d'un appareil comme cela a été présenté par certains (Perez, 2015), nous avons néanmoins à faire face à un problème sérieux engageant la sécurité des vols commerciaux. Des incidents du même type que le tailstrike du vol Emirates pourraient par exemple avoir lieu plus souvent si de nombreux pirates autour du globe décidaient de modifier les informations de masses reçues par les appareils au décollage.

Les possibilités réelles d'attaque dépendent de très nombreux facteurs, dont l'ingéniosité de pirates et de leurs connaissances des procédures classiques du contrôle aérien. Nous sommes convaincus que les menaces que nous avons détaillées sont crédibles parce certaines des circonstances nécessaires au déclenchement d'incidents ont déjà été réunies sans aucune intervention mal intentionnée. Nous sommes maintenant convaincus que certains facteurs peuvent être manipulés. Cela ne rendrait pas un incident systématique en cas d'attaque, mais rend plus probable la réunion de tous les prérequis à un incident.

Si nos travaux nous ont permis de trouver en quelques semaines des failles, nous sommes convaincus qu'une analyse plus fine des communications par liaison de donnée permettrait de dégager d'autres scénarios tout aussi préoccupants. Leur faisabilité technique reste à être démontrée, ce qui sera traité dans la prochaine partie.

CHAPITRE 5 ÉTUDE DE LA VIABILITÉ TECHNIQUE D'UNE ATTAQUE SUR DATALINK

Notre analyse de risques a conclu que les attaques les plus préoccupantes portaient sur l'authentification. En outre, les entretiens que nous avons eus avec des pilotes nous ont permis de détailler des scénarios crédibles d'attaques sur les communications ACARS et FANS1/A qui exploitent le manque d'authentification de ces protocoles.

Pour prouver la viabilité technique des attaques que nous venons de présenter, il est nécessaire de couvrir plusieurs points :

1. Il convient de confirmer le postulat selon lequel les capacités techniques et financières nécessaires pour mener une attaque active via l'envoi de faux paquets sont faibles. Une attaque n'est en effet possible s'il est aisé de forger les signaux nécessaires pour communiquer avec un appareil.
2. Une fois en possession de ce signal, il est nécessaire de confirmer son fonctionnement sur des systèmes réels. Seuls la réception et le décodage d'un signal forgé sur un USRP par des composants avionique *Commercial of the shelf* - COTS permettra de mener cette validation.

Il est donc maintenant nécessaire de développer les outils techniques nécessaires à cette attaque active en environnement de simulation. Ceci nous permettra de nous assurer qu'il est possible de mener une attaque sur les liaisons de données tout en respectant les cotations en termes de capacité faites dans l'analyse de risque.

Au cours du développement de la preuve de concept - POC, une attention particulière a été portée sur l'optimisation du coût ainsi que des connaissances. Si l'information est disponible sur Internet (et est donc publique), il est possible pour n'importe qui de l'acquérir, ce qui maintient au niveau le plus faible la capacité nécessaire à son obtention. En outre, toute organisation criminelle suffisamment motivée disposerait de quelques centaines de dollars qu'elle pourrait investir dans du matériel. Nous nous permettrons donc d'utiliser une radio logicielle - USRP B200 de la marque *Ettus Research* dont le coût est d'environ 1000 CAD. Si des radios logicielles bien moins dispendieuses sont disponibles sur le marché, elles se contentent généralement de la réception là où nous devons être en mesure d'émettre un paquet.

Notre POC se concentrera sur les messages ACARS pour plusieurs raisons. Cette technologie est la plus ancienne et est donc la plus utilisée (sur les réseaux ACARS historiques dans le cas

d'AOC ou VDL pour les opérations de contrôle). En outre, la majeure partie des appareils commerciaux possède le matériel nécessaire à l'utilisation d'ACARS ce qui rend la validation sur un aéronef réel plus aisé par la suite. Une démarche similaire pourrait dans tous les cas être adaptée à tous les protocoles de communications par liaison de données.

5.1 Création d'un signal ACARS

La preuve de concept d'attaque sur les liaisons de données ACARS repose sur deux parties complémentaires. Premièrement, un script permettra de générer rapidement des trames ACARS afin de pouvoir envoyer en temps réel des messages arbitraires à un aéronef particulier. Ce script doit nous permettre de renseigner tous les champs nécessaires pour l'adressage du message à l'acteur concerné et générer le message ACARS associé. Ce message sera ensuite modulé en MSK et envoyé via radio logicielle, selon les spécifications de la norme ARINC-618 (ARINC, 2016). Cette modulation est effectuée grâce à un schéma bloc sous Gnuradio (Hilburn and Corgan, 2017) et constitue la deuxième partie de la POC. Il s'agit d'un environnement de développement complet qui permet de contrôler une radio logicielle aisément.

La modulation MSK représente la difficulté technique principale pour la réalisation d'une attaque sur liaison de données. Nous avons implémenté directement dans Gnuradio une modulation qui respectait toutes les contraintes importantes pour la modulation MSK comme détaillée dans la partie 2.3 :

- Encodage NRZI,
- Baud de 2400,
- Fréquence de la pseudo-porteuse de 1800 Hz, donnant une fréquence basse de 1200 Hz et une fréquence haute de 2400 Hz.

Pour résumer le principe de fonctionnement de MSK, si deux bits successifs du message original sont les mêmes, la fréquence transmise est de 2400 Hz. À l'inverse, si deux bits successifs sont différents, la fréquence transmise est de 1200 Hz. Tant que le Baud est respecté et que le message envoyé est au bon format, l'avionique d'un avion commercial ainsi que les différents récepteurs disponibles sur le web devraient accepter tous les paquets transmis.

Il est possible de générer cette modulation de nombreuses manières différentes. Une première approche consiste à multiplier directement le signal carré à envoyer par les porteuses et pseudo-porteuses utiles dans le cas de MSK (Ziemer and Tranter, 2009). Nous avons dans un premier temps adopté cette méthode dans Simulink, un environnement de modélisation graphique de systèmes physiques développé par la compagnie TheMathWorks. comme présenté sur la Figure 5.1.

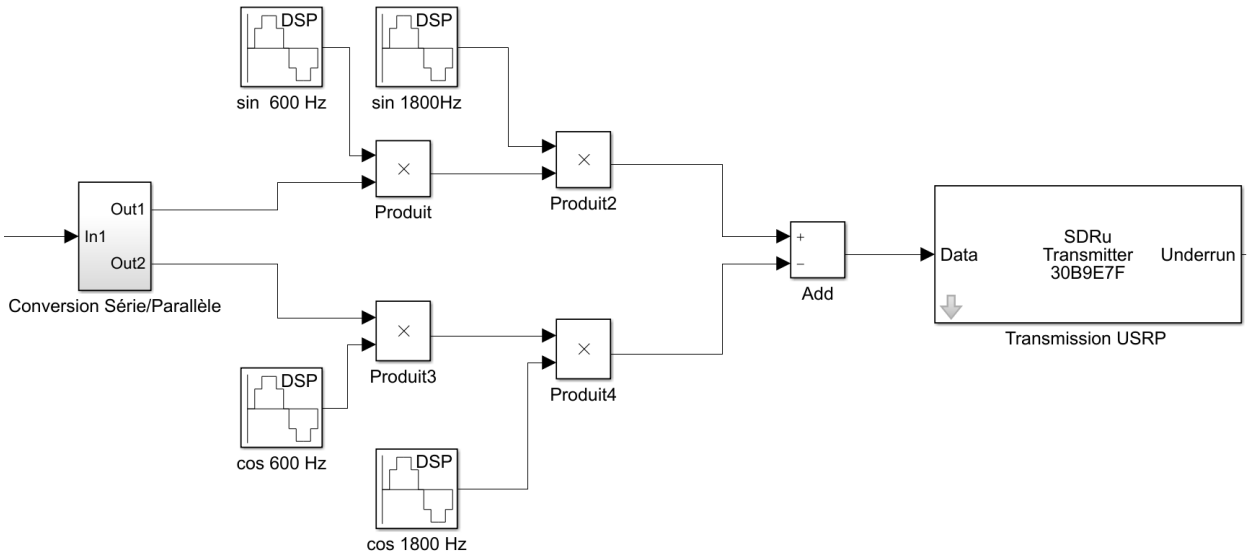


Figure 5.1 Implémentation directe du MSK dans Simulink

Si les résultats obtenus sont bons, ce procédé nécessite des ressources calculatoires élevées. Il est donc utilisable uniquement sur des ordinateurs dispendieux. Ceci est directement en contradiction avec la capacité faible que nous avons établie pour lancer une attaque. Nous pensons que ceci est en grande partie liée à la génération simultanée de 4 sinusoïdales à une fréquence d'échantillonnage de 50 000 Hz. Afin d'économiser les ressources du processeur, ce qui nous permettrait de lancer l'attaque depuis des machines moins performantes, nous avons choisi d'adopter une approche un peu plus fine.

La modulation MSK est maintenant directement implémentée sous Gnuradio, nous modifions le code binaire avant modulation afin de traduire directement les changements de bits. Deux bits successifs identiques seront traduits par un "0", et un changement de bit sera codé par un "1". Cette opération est aisément réalisée en effectuant une opération de "ou exclusif" entre le paquet original et le même message décalé d'un bit. Ces opérations sont détaillées à la figure 5.2

Il suffit ensuite d'appliquer une modulation en fréquence adaptée au signal prétraité. La sensibilité ainsi que le facteur d'interpolation sont choisis afin d'avoir un Baudrate adapté de 2400. Il ne reste alors qu'à appliquer une ultime modulation de fréquence selon la bande d'émission désirée telle que celles présentées dans le tableau 5.1.

Tableau 5.1 Quelques fréquences ACARS - (ARINC, 2016)

Fréquence - MHz	**Utilisation**
131.450	Fréquence japonaise principale
131.550	Fréquence mondiale principale
131.725	Fréquence européenne principale
136.775	Fréquence russe principale

5.2 Utilisation du signal sur des systèmes réels

Dans un premier temps, le fonctionnement de cette preuve de concept a été vérifié grâce à des décodeurs open source. Nous avons soumis les paquets forgés à tous les récepteurs utilisés lors de l'interception des paquets au début de nos recherches. Il est strictement illégal de procéder à l'émission de signaux dans ces bandes de fréquences sans une licence aéronautique dédiée. Nous avons donc connecté notre USRP B200 en émission à une SDR classique de la marque nooelec via un câble. Cela prévient toute émission réelle de paquet ACARS malicieux. Une fois que l'USRP émet les paquets forgés, le signal est reçu par la SDR et démodulé puis décodé par différents logiciels libres, comme présenté à la figure 5.3. Nous avons ainsi pu décoder notre signal grâce à l'outil *acarsdeco* (Tomsk State University of Systems Control and Radioelectronics, 2016), un logiciel de décodage de signaux ACARS libre de droits, et au module *acars2*, qui fait partie des librairies standard du projet gnuradio. L'envoi de paquets est fait en boucle afin de nous assurer de la réception. En condition d'utilisation normale, à moins de vouloir brouiller la fréquence, les paquets seraient transmis une seule fois.

La preuve de concept telle que nous l'avons développée est totalement adaptée à une attaque sur les vitesses au décollage. Un attaquant avec les mêmes résultats pourrait aisément transmettre de fausses informations à un appareil encore au sol en utilisant les bandes VHF. En écoutant quelques minutes les échanges sur la fréquence dédiée aux communications AOC, il serait possible de relever l'immatriculation d'un appareil sur le point de partir. Suite à l'envoi des données de masses à sa compagnie, il suffirait de répondre avec un message au même format comprenant des données de vitesse arbitrairement modifiées. Le recourt à un script python similaire à celui que nous avons utilisé permet de forger des messages malveillants en quelques secondes et donc de répondre rapidement à l'avion ciblé.

Afin de confirmer définitivement leur efficacité, une étape nécessaire aurait été leur émission vers les composantes avioniques d'un avion de ligne. Malheureusement, à cause des nombreuses contraintes, il n'a pas été possible de réaliser ce test. En effet, les composantes avioniques COTS sont très dispendieuses et il est difficile de nous en procurer. Les avions de lignes qui en possèdent sont sans cesse soumis à des opérations de maintenance et d'exploi-

tation qui rendent difficile leur immobilisation à des fin de tests. Enfin, il est interdit à moins de disposer d'une licence appropriée d'émettre un signal sur les fréquences aéronautiques, ce qui aurait nécessité un environnement de test fortement contrôlé.

Néanmoins, nous ne présentons que peu de réserves concernant leur fonctionnement sur de l'avionique COTS. En effet, l'acceptation par les décodeurs open source nous permet de valider l'efficacité de notre modulation MSK. Ces derniers ont été développés pour recevoir des signaux issus de composantes avioniques commerciales classiques, ce qui indique la forte similarité entre nos paquets et les trames réelles. De plus, il n'y a dans le protocole ACARS aucun contrôle de numéro de séquence ou d'origine qui pourrait invalider un paquet, tant que les champs d'adressage sont correctement renseignés. Bien que nous ne l'ayons pas développé, une approche tout à fait similaire est envisageable concernant les communications CPDLC et ACARS sur VDL.

5.3 Synthèse des requis à une attaque sur ACARS

Nous avons obtenu les outils nécessaires à l'élaboration d'une attaque sur ACARS grâce à la création d'un signal radio légitime et à son envoi. Nous sommes dorénavant en mesure de dresser avec précision la liste du matériel ainsi qu'une idée du temps nécessaire au développement de cette attaque :

1. Une USRP B200 de la marque Ettus Research (ou matériel équivalent) pour l'émission du signal a un coût d'environ 1000 CAD.
2. Une SDR NESDR de la marque NooElec (ou matériel équivalent) pour la réception des paquets et le débogage lors du développement, à un coût d'environ 20 CAD.
3. La suite logicielle libre Gnuradio ainsi que le module acarsdeco2 disponibles gratuitement pour la modulation MSK et la communication avec l'USRP et la SDR.
4. Un logiciel libre de décodage de signaux ACARS tel que acarsdec.
5. Entre 160 et 200 heures de travail pour l'intégration et les tests avec une personne de niveau technique ingénieur et aucune connaissance préalable des systèmes de communication par liaison de données.

Le temps de travail nécessaire au développement de cette preuve de concept représente environ le fruit d'un mois de travail à plein temps pour un ingénieur. Le principal obstacle à l'obtention de notre attaque a été la collecte des informations nécessaire à sa mise en place. ACARS est une technologie propriétaire et son standard est vendu à un prix élevé. Néanmoins, plusieurs publications universitaires détaillent une partie des informations utiles

pour la création d'un signal viable. La collecte et la vérification de ces sources demandent de nombreuses heures de travail.

Il est ensuite aisé de coder un script nécessaire à la création d'un paquet arbitraire en quelques secondes tant que le format d'une trame ACARS est respecté, et la modulation MSK est très bien détaillée dans de nombreux ouvrages ainsi que sur Internet. Ainsi, une fois passée la période de prise en main de gnuradio, peu de temps est nécessaire afin de répliquer une modulation telle que MSK grâce aux outils natifs de gnuradio.

De fait, bien qu'elle soit encore incomplète, car nous n'avons pas réalisé de tests sur de véritables composants avioniques, nous avons jusqu'à un certain point prouvé la viabilité technique d'une attaque sur les communications par liaison de données. Nous faisons maintenant face à des scénarios d'attaque crédibles, aisément exploitable avec des moyens limités et à la portée de nombreux acteurs. Il ne subsiste plus aucun doute quant à la nécessité de l'utilisation de solutions cryptographiques visant le maintien de l'intégrité et permettant l'authentification des paquets échangés par liaison de donnée.

Comme nous l'avons déjà vu, si de telles solutions existent, elles ont été développées dans un contexte différent de celui de l'aéronautique commerciale. Il est maintenant nécessaire de vérifier dans quelle mesure les standards de sécurisation comme AMS sont pertinents pour une utilisation civile.

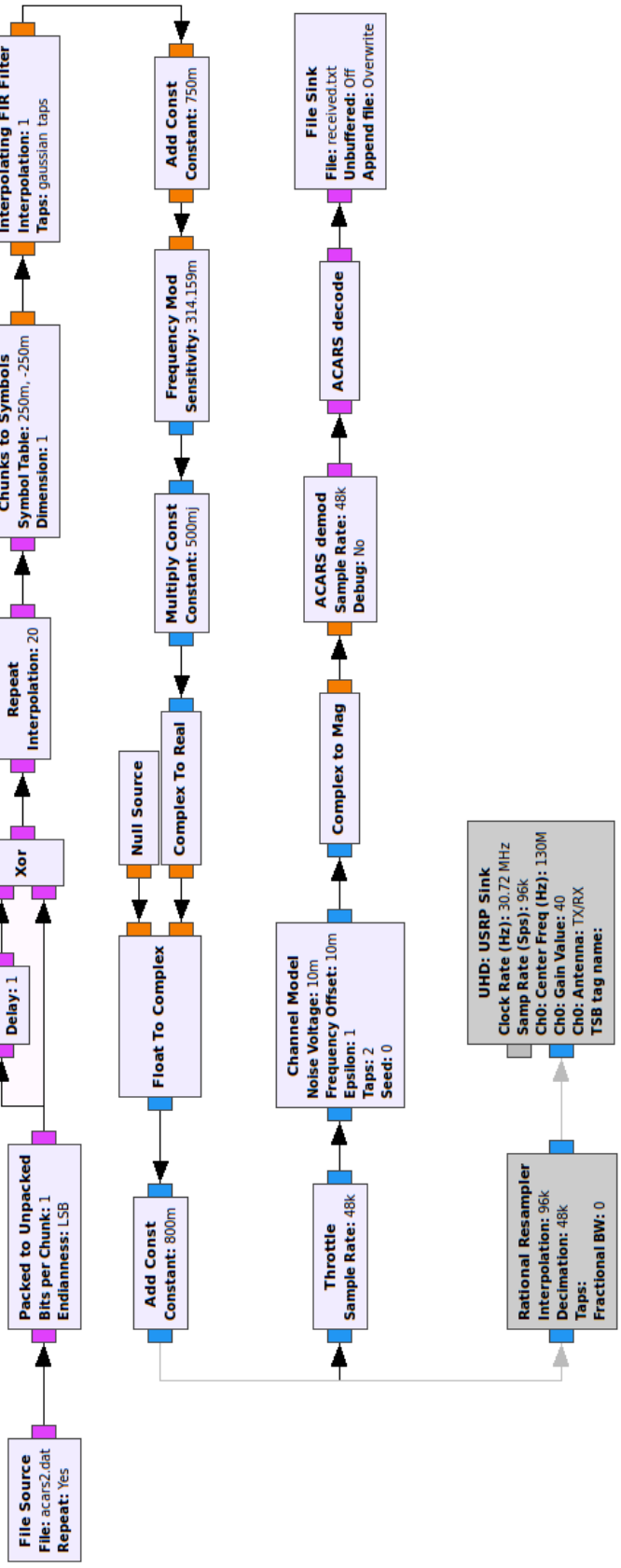


Figure 5.2 Diagramme GNU radio de modulation MSK

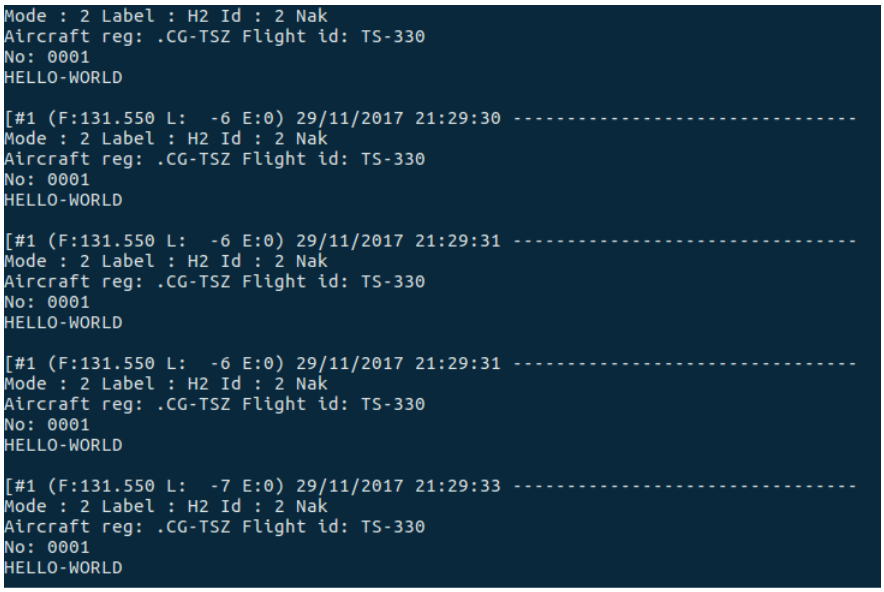


Figure 5.3 Réception de paquets forgés

CHAPITRE 6 VIABILITÉ DE L'UTILISATION GÉNÉRALISÉE D'AMS POUR L'AVIATION CIVILE

Nous l'avons vu, des versions sécurisées des communications ACARS existent déjà. Néanmoins, l'utilisation de méthodes comme celles proposées par ARINC-823 entraîne systématiquement une augmentation de la taille des paquets, ainsi que leur nombre (ARINC, 2007). La mise en place de 6 nouveaux messages est par exemple nécessaire afin d'initialiser ou de mettre fin à des sessions sécurisées. En outre, les différents algorithmes cryptographiques utilisés entraînent une augmentation de la taille des paquets eux-mêmes, le plus souvent via l'ajout des données nécessaires à l'authentification d'un paquet.

Il apparaît rapidement que la quantité totale du trafic augmentera suite à l'utilisation massive de méthodes cryptographiques comme proposées par AMS. Il convient d'évaluer si l'utilisation généralisée de telles méthodes à tous les appareils en vol est possible sur le réseau actuel, ou si le risque de congestion est trop important. Il est également nécessaire de nous assurer qu'AMS est compatible avec les nombreux systèmes déjà en place et que son utilisation ne pose aucun problème de rétrocompatibilité.

Dans un premier temps, nous allons tenter d'estimer l'utilisation actuelle des réseaux ACARS dans une zone aéroportuaire (puisque c'est ici que l'utilisation des fréquences sera maximale). Cela permettra par la suite d'obtenir une idée de l'évolution de la quantité de données échangées en cas de recourt généralisé à des solutions cryptographiques, ainsi que la marge de manœuvre disponible.

Nos estimations sont basées sur l'écoute de messages ACARS transitant sur le réseau historique associé (et non VDL). L'impact sur les paquets ACARS sur FANS1/A serait néanmoins le même. En effet, si les paquets sont encapsulés dans des trames compatibles à une utilisation sur VDL, elles contiennent un unique paquet ACARS (ARINC, 2016). La troncature d'un paquet ACARS sur VDL résulterait donc en 2 messages transmis sur le réseau. En outre, nous nous concentrons uniquement sur les communications ACARS sur le réseau dédié VHF (non VDL) car il est aujourd'hui le plus à même de présenter des risques de congestion. En effet, ces réseaux étant les plus anciens, la gestion qui y est faite dans la bande passante est la moins optimale.

6.1 Charge observée des réseaux ACARS

Il n'existe pas à notre connaissance de bases de données publiques de messages ACARS. Afin de contourner ce problème, nous avons décidé de recueillir nous-mêmes des échanges ACARS sur plusieurs semaines. Nous avons placé un Raspberry pi 3 et une SDR en ligne de vue sur l'aéroport de Montréal Pierre-Elliot Trudeau dont le code IATA est YUL. Le logiciel acarsdeco a été lancé en écoute continue pendant 28 jours, du 7 décembre 2017 au 3 Janvier 2018, ce qui nous a permis de récupérer les échanges entre appareils, centre de contrôle et opérations des compagnies aériennes de la zone. La fréquence écoutée était 131.550 Mhz, la fréquence ACARS mondiale principale.

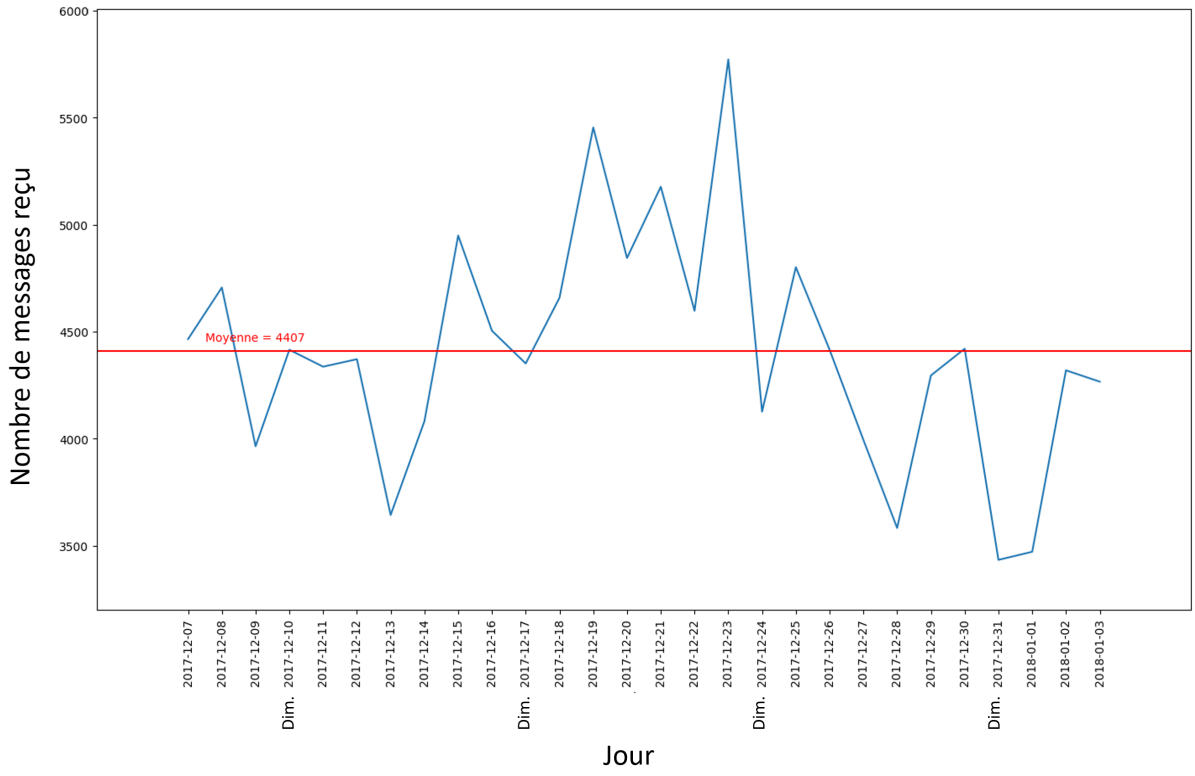


Figure 6.1 Nombre de messages reçus par jour sur la fréquence 131.550 Mhz à YUL

Le compte des messages reçus par notre installation chaque jour, ainsi que la taille des paquets offre de précieuses informations sur l'utilisation du réseau. Il est possible d'évaluer son utilisation moyenne grâce à ces données. Un total de 123 409 échanges ont été interceptés au cours des 28 jours ce qui représente une moyenne d'environ 4 407 messages par jour, soit un paquet transmis toutes les 19,6 secondes0. La longueur moyenne du texte transmis est de 22 caractères, auxquels il faut ajouter les 48 caractères nécessaires lors de l'envoi d'un paquet

vide. Les paquets ACARS que nous avons reçus ont donc une taille moyenne de 70 caractères, ou encore 560 bits. Transmis à un débit de 2400 bits par secondes, la durée moyenne d'un paquet ACARS est donc de 0,23 seconde.

L'accès au réseau est régulé par CSMA ce qui nous permet de mettre de côté l'éventualité de collisions. Le réseau ne sera saturé que si l'attente avant d'être en mesure d'émettre un paquet est longue, et non pas si trop de collision apparaissent sur le réseau. En considérant que le trafic est équitablement réparti sur toute la journée, l'envoi d'un message d'une durée de 0,23 seconde toutes les 19,6 secondes représente une utilisation du réseau de 1,17%. Nous sommes en apparence très loin des limites autorisées par le réseau ACARS.

Néanmoins, une telle analyse n'est représentative de l'utilisation réelle des réseaux de liaison de données :

1. Tous les messages transmis n'ont probablement pas pu être reçus. L'antenne utilisée n'est pas parfaitement adaptée à la réception à 131.550 Mhz et son gain n'est pas optimal à la fréquence étudiée. Il est donc possible que la durée moyenne entre l'émission de deux paquets soit inférieure aux 19,6 secondes calculées.
2. La météo est également un facteur influant grandement la propagation des ondes radio. On s'attend par exemple à plus de pertes les jours de mauvais temps, puisque les précipitations dégradent les performances de réception radio. Il est intéressant de relever au contraire que les jours de météo défavorable correspondent à des maximums de réception de messages (notamment le 23 décembre ou de fortes chutes de neige ont eu lieu). Ceci s'explique par les nombreux rapports D-ATIS émis par la tour de contrôle pour informer les pilotes de l'état dégradé des pistes ce jour-là.
3. On a supposé que les émissions sont réparties uniformément dans le temps ce qui est faux. Il convient d'étudier la répartition au cours d'une journée de l'envoi des paquets ACARS afin de voir si le réseau approche de sa limite aux heures de pointe ou non.
4. Si le débit théorique d'ACARS est de 2400 bit/s, ce n'est pas le cas en pratique. Les réseaux ACARS imposent aux appareils qui les utilisent une méthode d'accès de type Carrier Sense Multiple Access (CSMA). Dans ce type de réseau, le débit maximal réel est d'environ 40% du débit maximal théorique (Kleinrock and Tobagi, 1975).

Il est possible d'affiner légèrement les résultats obtenus précédemment via le tracé heure par heure des messages reçus par la SDR au cours des 28 jours, comme montrés sur la figure 6.2. Les échanges ACARS reçus présentent une forte corrélation avec le nombre d'appareils entrant ou sortant de la zone de contrôle de l'aéroport YUL. On constate donc une augmentation du trafic au cours de la journée et une diminution la nuit. Chaque jour, 308 messages en moyenne

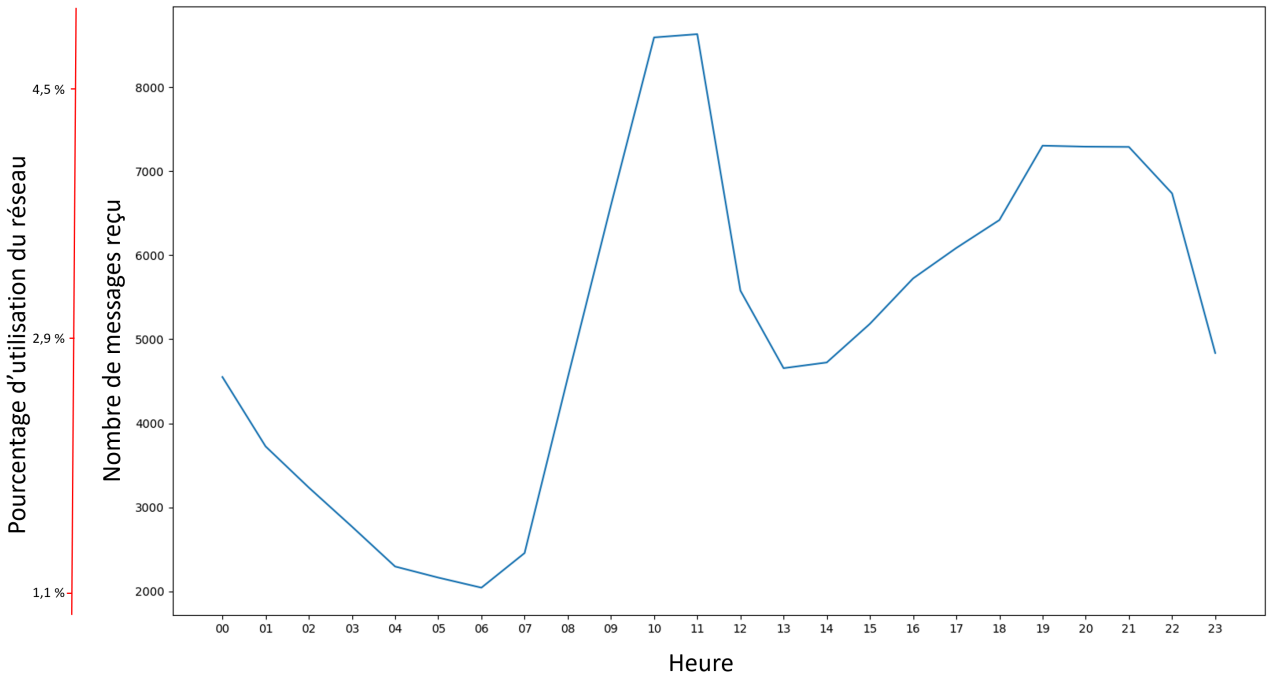


Figure 6.2 Nombre de messages reçus par heure sur la fréquence 131.550 Mhz à YUL - Somme sur 28 jours. Capacité maximale corrigée à 40% de la capacité maximale théorique.

ont été reçus entre 11h et midi. Nous constatons que même aux heures de pointe, l'utilisation maximale qui est faite du réseau reste très faible par rapport à sa capacité maximale et ne dépasse que de peu les 4,5%, rapportés à la capacité maximale réelle du réseau qui est de 40% de sa capacité maximale théorique.

Bien que la distribution de l'envoi de paquets ne soit pas uniforme, les résultats de la figure 6.2 nous permettent d'affirmer qu'on n'attend pas une grosse différence entre la moyenne par heure, minute ou seconde de la quantité de trafic sur le réseau ACARS.

6.2 Augmentation du trafic causée par AMS

L'aéroport YUL est de taille modeste par rapport aux grandes plaques tournantes aériennes comme Atlanta, London Heathrow, etc. Il convient de vérifier dans quelle mesure nos résultats sont applicables à ces aéroports au trafic bien plus important.

En outre, l'impact sur la quantité totale de trafic des méthodes cryptographiques est encore inconnu. Nous relevons deux sources principales dans l'augmentation de la quantité de paquets sur le réseau. La première est l'ajout des données nécessaires à l'authentification des

paquets (HMAC ou signature numérique). En outre, les handshakes qui n'existent pas sans AMS causent également l'envoi de nouveaux paquets jusqu'alors inexistants. En considérant que la majeure partie des paquets transmis sont des paquets de tests, il est raisonnable de considérer que chaque nouveau paquet a une taille de 70 caractères, ce qui est la taille moyenne qui a été observée sur le réseau. Il est possible de quantifier le nombre total de paquets envoyés sur le réseau avec l'utilisation d'AMS grâce à la formule :

$$X_{tot} = P + T + H$$

Où X_{tot} représente le nombre de messages envoyés sur le réseau si utilisation d'AMS. T représente le nombre de paquets qui auraient été troncaturés sur les 28 jours à cause de l'ajout d'un HMAC, P représente le nombre de messages reçus (123 409) et H représente le nombre de paquets qui auraient été nécessaires à la mise en place de sessions sécurisées.

En gardant les mêmes notations, l'augmentation en pourcentage du trafic sur le réseau causé par AMS notée Δ_{AMS} vaut :

$$\Delta_{AMS} = \Delta_{HMAC} + \Delta_{Handshake} = \frac{T * 100}{P} + \frac{H * 100}{P}\%$$

6.2.1 Impact du HMAC

Le HMAC qui est ajouté à la fin des messages occupe une taille minimale de 32 bits (soit 4 caractères). La taille de ce champ supplémentaire peut être augmentée à 128 bits afin de garantir une meilleure sécurité. Pour que les trames sécurisées soient correctement reçues par le matériel déjà déployé dans les avions et au sol, on ne peut ajouter de champ supplémentaire à ACARS. Les informations du HMAC doivent donc être ajoutées à la fin du paquet, et occupent des octets qui étaient jusqu'alors réservés au *free text*, pour lequel 220 caractères sont réservés en uplink et 210 en downlink.

Dans le premier cas, un HMAC ne laisserait plus que 204 à 216 caractères de texte disponibles, selon le niveau de sécurité désiré. Tous les messages ayant une taille supérieure à la nouvelle limite imposée devraient donc être coupés en deux.

La plupart des paquets reçus sont vides ou sont des messages tests, mais les plus volumineux ayant une payload comprise entre 204 et 219 caractères devront être coupés et causeront l'apparition d'un nouveau paquet. Nous ne comptons pas les paquets de 220 caractères free text exactement, car nous supposons qu'ils ont déjà été coupés. En résumé, comme indiqué à la figure 6.3 :

— Entre 0 et 204 caractères, le HMAC n'a aucun impact sur le paquet
— Entre 204 et 219 caractères, en fonction de la taille choisie pour le HMAC, le paquet devrait être découpé en deux.
— Si le paquet fait 220 caractères, on considère qu'il a déjà été découpé en plusieurs messages et le HMAC n'est donc pas la cause directe de la troncature.

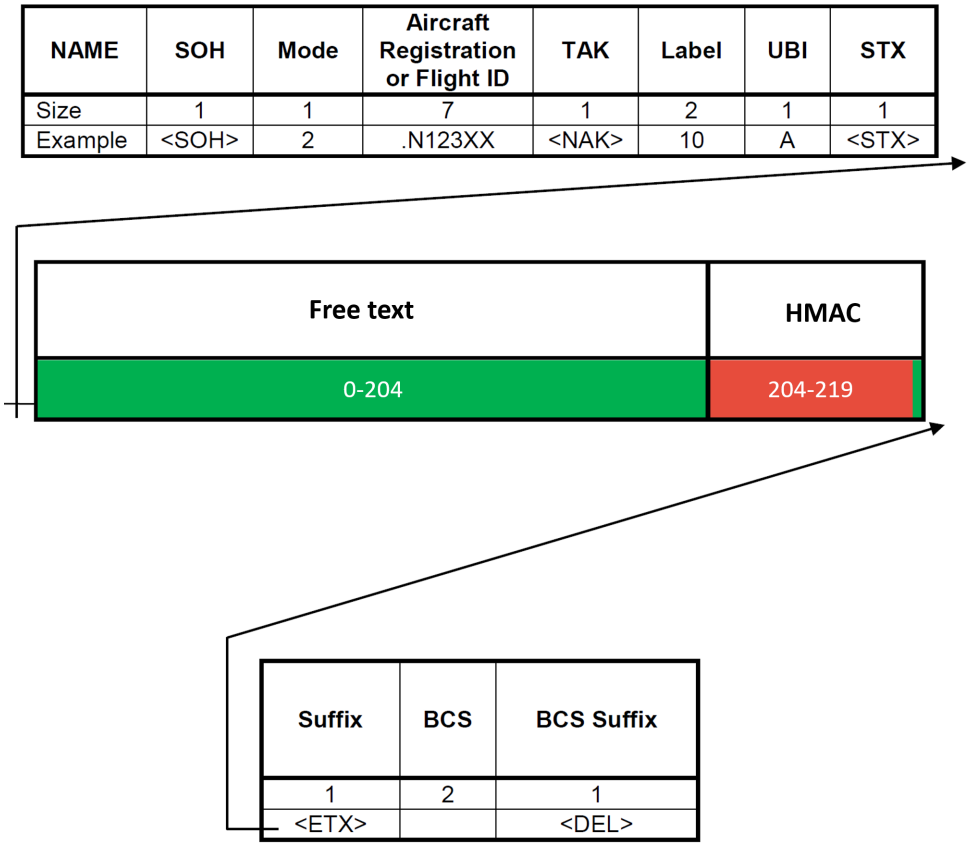


Figure 6.3 Trame AMS avec ajout d'un HMAC (ARINC, 2016) (ARINC, 2007)

Les modifications dans la quantité de trafic induites par la troncature en deux des messages dépassant respectivement 204, 212 et 216 caractères sont indiquées dans le tableau 6.1.

Tableau 6.1 Augmentation du trafic ACARS en fonction de la taille du HMAC

Taille du HMAC	**Messages tronqués**	**Augmentation du trafic - Δ_{HMAC}**
32 bits - 4 caractères	20	0.016 %
64 bits - 8 caractères	256	0.21 %
128 bits - 16 caractères	1671	1.35 %

L'impact sur le réseau de ce champ supplémentaire est négligeable face aux échanges déjà existants, car la plupart des paquets ACARS contiennent peu de texte et ils ne seront donc pas coupés en deux. La figure 6.5 présente une boite à moustache de la taille des paquets reçus chaque jour de la collecte des paquets et présente la faible quantité de paquets concernés. L'ajout du HMAC est donc tout à fait envisageable aujourd'hui. Des HMAC de grande taille ne causeraient pas non plus de dégradation des performances du réseau préjudiciable à son fonctionnement. Néanmoins, le code d'authentification n'est pas le seul facteur pouvant modifier la quantité de messages de liaison de données.

6.2.2 Impact des handhsakes

Des messages, au nombre de six, jusqu'alors inexistants sont nécessaires au calcul et à la transmission des clés partagées utilisées par les différents algorithmes cryptographiques proposés par AMS. Seuls cinq sont utilisés par les handshakes qui permettent la mise en place et la fin d'une session sécurisée :

- *Initialization_indication*
- *Initialization_request*
- *Initialization_response*
- *Session_release_request*
- *Session_release_response*

Au cours des 28 jours et en moyenne, 92,25 appareils uniques ont utilisé chaque journée la fréquence 131.550 Mhz pour envoyer des paquets ACARS comme montré à la figure 6.4. Il est alors possible d'obtenir un ordre de grandeur du nombre d'appareils différents qui échangent des messages ACARS à l'aéroport de Montréal. Chaque appareil entrant sur cette fréquence causerait l'envoi de 5 paquets supplémentaires nécessaires à la mise en place des sessions sécurisées AMS, soit $H = 12\ 943$ paquets supplémentaires sur la durée totale d'observation. En comparaison avec les 123 409 reçus pendant nos 28 jours, cela représenterait une augmentation de 10,5% des échanges sur le réseau.

On a en reprenant la notation précédente :

$$\Delta_{Handshake} = \frac{H * 100}{P} = 10,5\%$$

L'augmentation totale dans le nombre de paquets envoyés lié à l'ajout des mesures cryptographiques d'AMS est donc de :

$$\Delta_{AMS} = \begin{cases} 10,516\%, & \text{si taille HMAC} = 32 \text{ bits} \\ 10,71\%, & \text{si taille HMAC} = 64 \text{ bits} \\ 11,85\%, & \text{si taille HMAC} = 128 \text{ bits} \end{cases}$$

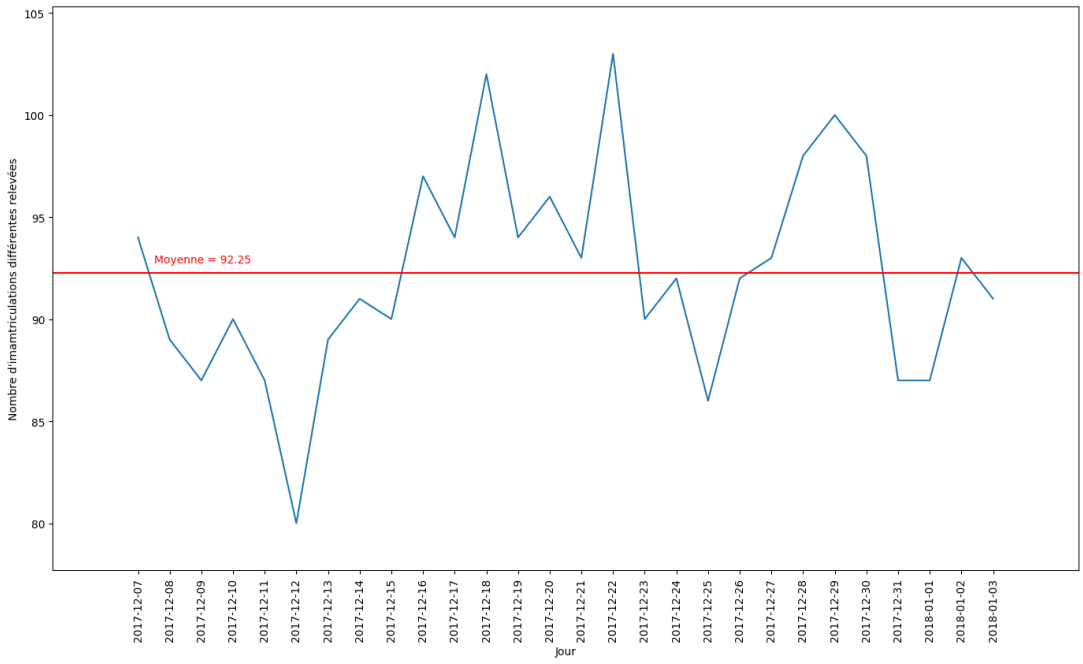


Figure 6.4 Nombre d'immatriculations uniques reçues chaque jour à YUL

6.3 Optimisations possibles

L'augmentation naturelle du trafic aérien est estimée entre 1,6% et 3,9% (Gregorova, 2010). La mise en place et l'utilisation par les avions commerciaux d'AMS conduiraient donc à une perte de l'équivalent de 2 à 6 ans d'exploitation du réseau selon nos prédictions les plus pessimistes. Ces chiffres sont probablement légèrement plus faibles en réalité, car les appareils commerciaux sont dotés de plus en plus de composantes avioniques, qui nécessitent de communiquer avec le sol, et qui causent l'envoi de message de plus en plus nombreux.

Le réseau sera considéré comme congestionné lorsque cette attente sera trop longue, ce qui correspond comme nous l'avons vu à une utilisation d'environ 40% de la capacité théorique

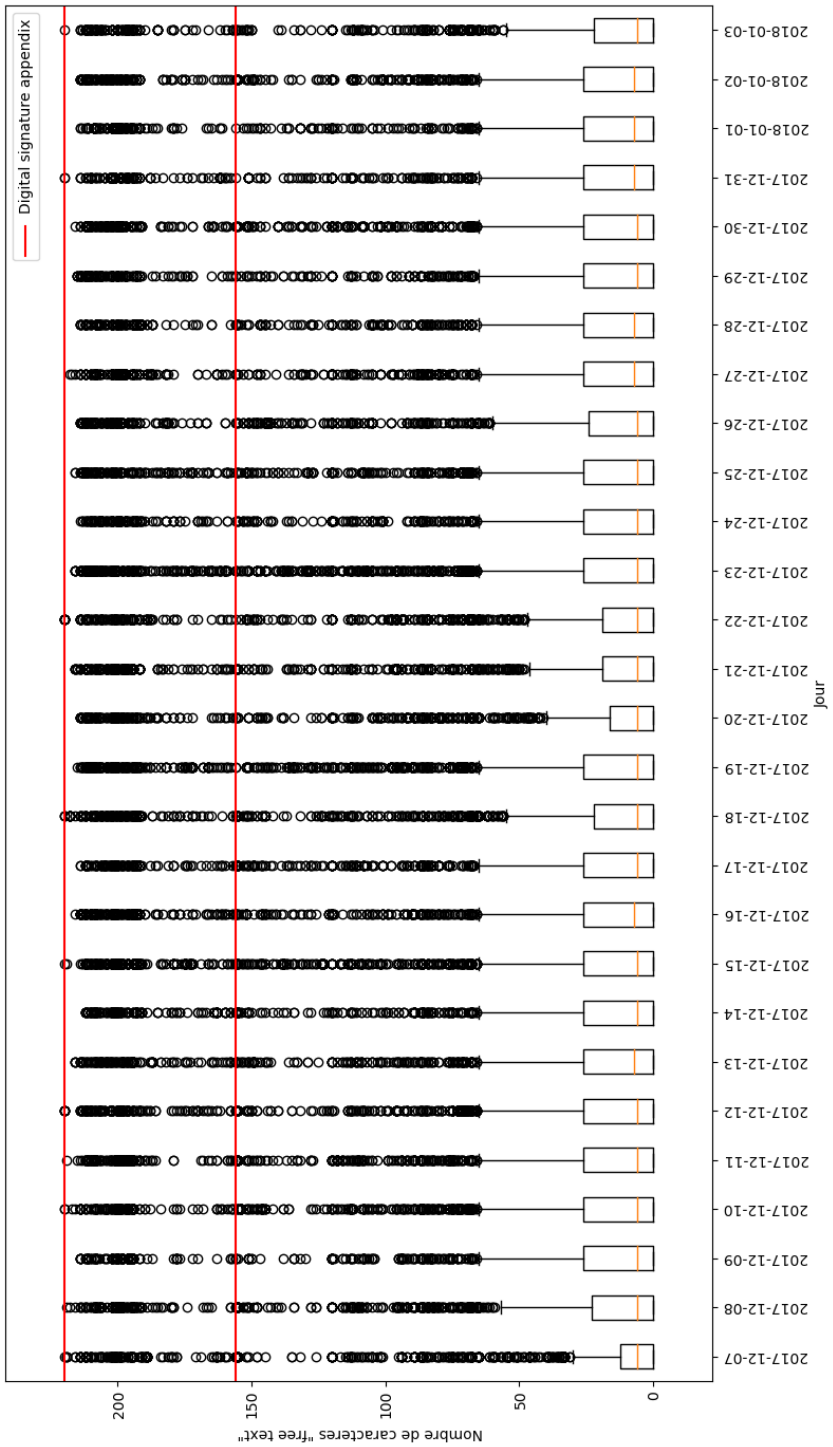


Figure 6.5 Taille du texte inclus dans les messages ACARS reçus, boites à moustache

maximale. Dans les zones aéroportuaires à faible trafic aérien, une fois que nous nous sommes ramenés à la véritable limite du système, l'utilisation faite du réseau ACARS est d'environ 4,5% de sa capacité maximale.

D'après les données du conseil International des Aéroports - ACI, YUL a enregistré 235 099 mouvements d'appareils l'année dernière. L'aéroport d'Atlanta de code IATA ATL/KATL qui est le plus occupé au monde a enregistré environ quatre fois plus de trafic avec 883 680 mouvements d'avions. Sous l'hypothèse que l'utilisation des fréquences ACARS qui y est faite est proportionnelle à la quantité d'appareils en circulation, on pourrait donc s'attendre à des réseaux quatre fois plus occupés, soit à environ 18% de leur capacité maximale.

Sous l'hypothèse qu'elle soit linéaire, une croissance de 3,9% par an du trafic aéroporté laisse une marge de 21 ans avant la congestion du réseau au niveau des plus grands aéroports. D'après nos estimations présentées à la figure 6.6, dans le plus pessimiste des scénarios, les réseaux ACARS seraient congestionnés autour de l'année 2040. Cette hypothèse de linéarité est à nuancer, car les appareils commerciaux ont tendance à embarquer de plus en plus de composantes avioniques qui ont besoin des systèmes Datalink afin de mettre en place des communications air-air et air-sol.

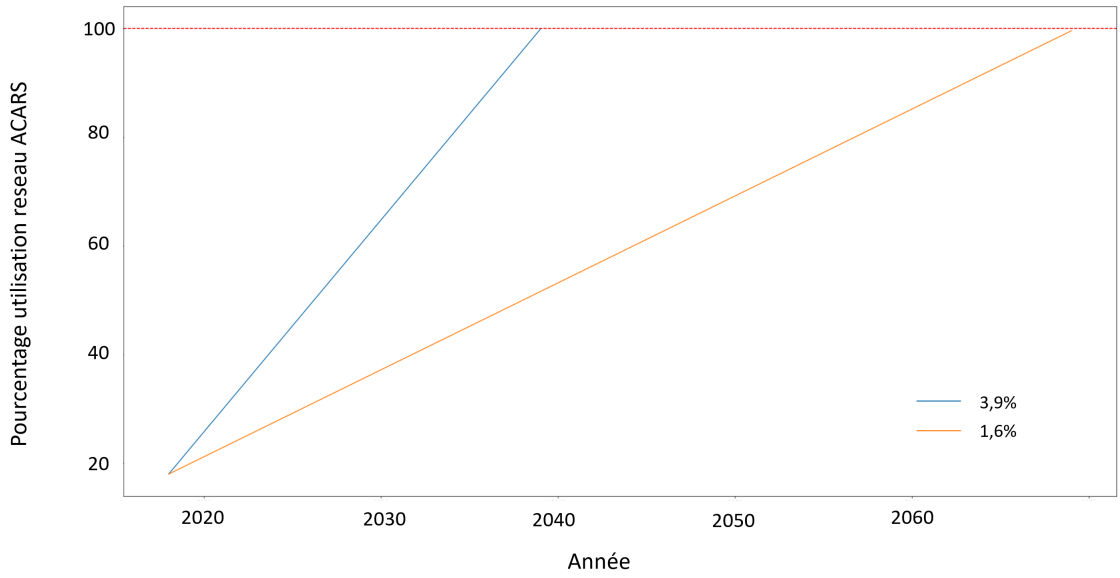


Figure 6.6 Prévision de l'utilisation des réseaux ACARS dans les grands aéroports. La courbe bleue représente l'évolution du trafic ACARS si le trafic aérien connaît une croissance de 3,9% par année, la courbe orange sous une croissance de 1,6% par an.

Il est possible de proposer des pistes d'améliorations dans les performances d'AMS à condition d'apporter des modifications au protocole. Cette démarche aboutirait à la rédaction d'un

nouveau standard. La cause principale d'augmentation des échanges sur le réseau est liée à la mise en place des handshakes. Ces derniers sont nécessaires pour le calcul d'une clé partagée qui assurera par la suite la confidentialité via AES et l'authentification grâce à un HMAC.

Néanmoins, la confidentialité n'est pas un facteur vital dans les échanges ACARS des appareils commerciaux contrairement aux attentes des appareils militaires. En effet, l'interception et la compréhension des paquets seules ne peuvent permettre à un attaquant de mener une attaque avec un fort impact sur le réseau. Ce sont, nous l'avons vu, les attaques par usurpation qui sont les plus dangereuses. En d'autres termes, l'intégrité et l'authentification sont les objectifs de sécurité prioritaires, et ils peuvent être assurés via le recours à une signature digitale uniquement. Un paquet non ou mal authentifié devrait être simplement rejeté par l'avionique et ne pourra donc pas interférer avec l'appareil ou influencer le pilote dans ses décisions.

Dans une version uniquement authentifiée d'AMS, chaque paquet devrait être signé avec une signature numérique. C'est ce qui est déjà proposé dans les messages sans session (*Initialization_request*, *Initialization_response*, *Session_release_request* et *Session_release_response*). Une signature de 64 caractères ECDSA est ajoutée à la fin du message. Cependant, cela réduit de manière importante la charge utile du paquet concerné qui ne peut plus contenir que 146 caractères en downlink et 156 en uplink. Néanmoins, même avec une payload réduite de cette manière, peu de messages se retrouveraient troncaturés car, nous l'avons vu, un nombre très limité de paquets ont une taille importante.Un nouveau standard basé sur ARINC 823 pourrait donc apporter une meilleure utilisation de la bande passante disponible. Les handshakes non nécessaires ne seraient plus un problème et la diminution de la payload n'est pas problématique. Nous proposons donc les pistes d'ajustement suivantes :

6.3.1 Mode *Authenticated uplink*

Afin d'éviter les messages de handshake, il est possible d'utiliser une signature numérique sur les messages critiques uniquement. Cela est possible si nous ciblons uniquement un certain nombre de paquets importants grâce à leur étiquette (champ *label*). C'est par exemple le cas des instructions envoyées par les contrôleurs ou les opérations (étiquette C1 *uplink messages to the cockpit printer* ou H1 *terminal communication* par exemple).

La Figure 6.7 présente une classification des différentes étiquettes reçues lors de notre capture de nombreux paquets. La plupart des messages reçus sont des tests et des requêtes de changement de fréquence qui ne sont donc pas critiques et qu'il serait inutile d'authentifier. L'authentification des paquets C1 et H1 causerait une augmentation de 0,65% du trafic sur

le réseau. Une augmentation légèrement plus importante serait à prévoir si les trames jugées critiques possèdent d'autres labels en plus des deux que nous avons étudié.

Une telle approche permettrait de réduire de manière efficace les attaques sur les communications ATC, car la légitimité de chaque instruction reçue pourrait être vérifiée. Les certificats nécessaires à la vérification des clés publiques pourraient être rendus disponibles sur une base de données. Les pilotes devraient récupérer pendant la préparation de leur vol les informations nécessaires à l'authentification des centres de contrôle à rencontrer sur leur route. Cette solution serait viable, car un appareil traverse rarement un nombre très élevé de zones de contrôle différentes. En outre, un appareil aura tendance à effectuer de manière régulière certains trajets et n'aura pas besoin de toujours récupérer de nouveaux certificats qui pourraient être valables pour une période temporelle importante.

Ce mode laisserait une marge de manœuvre restreinte aux pirates pour lancer des attaques d'usurpation. Un choix judicieux des types de messages à sécuriser augmenterait considérablement la sécurité tout en minimisant l'impact sur le réseau des contre-mesures cryptographiques.

6.3.2 Mode *Fully authenticated*

Un mode *Fully authenticated* permettrait également aux appareils de signer les paquets transmis vers le sol. Cela réduirait drastiquement le risque en rendant impossible, par exemple, une attaque sur les vitesses V au décollage que nous avons déjà détaillé.

Il serait dans ce cas difficile de créer une base de données unique contenant les certificats de tous les appareils commerciaux et de les distribuer aux bons utilisateurs. Une solution alternative serait l'envoi par chaque appareil de son certificat lors d'un changement d'autorité de contrôle afin de pouvoir valider l'authenticité de tous les messages suivants. L'ajout d'une signature numérique de 64 caractères dans chaque paquet ACARS ainsi que l'envoi de 92,25 messages de certificats supplémentaires par jour (un par appareil) causerait une augmentation de 6,61% du trafic par rapport à notre jeu de données.

Ce mode présente des inconvénients tant sur l'utilisation du réseau que des ressources calculatoires fournies par l'avionique. Contrairement au *Authenticated uplink*, tous les paquets seraient signés et les vérifications de signature plus fréquentes. Ceci demande du temps supplémentaire et mettra plus à contribution les ressources calculatoires limitées des appareils en vol. Il conviendrait de vérifier que les matériels déjà implémentés dans les avions commerciaux seraient capables de vérifier régulièrement des signatures digitales sans que cela cause de ralentissement dans les autres tâches nécessaires au vol.

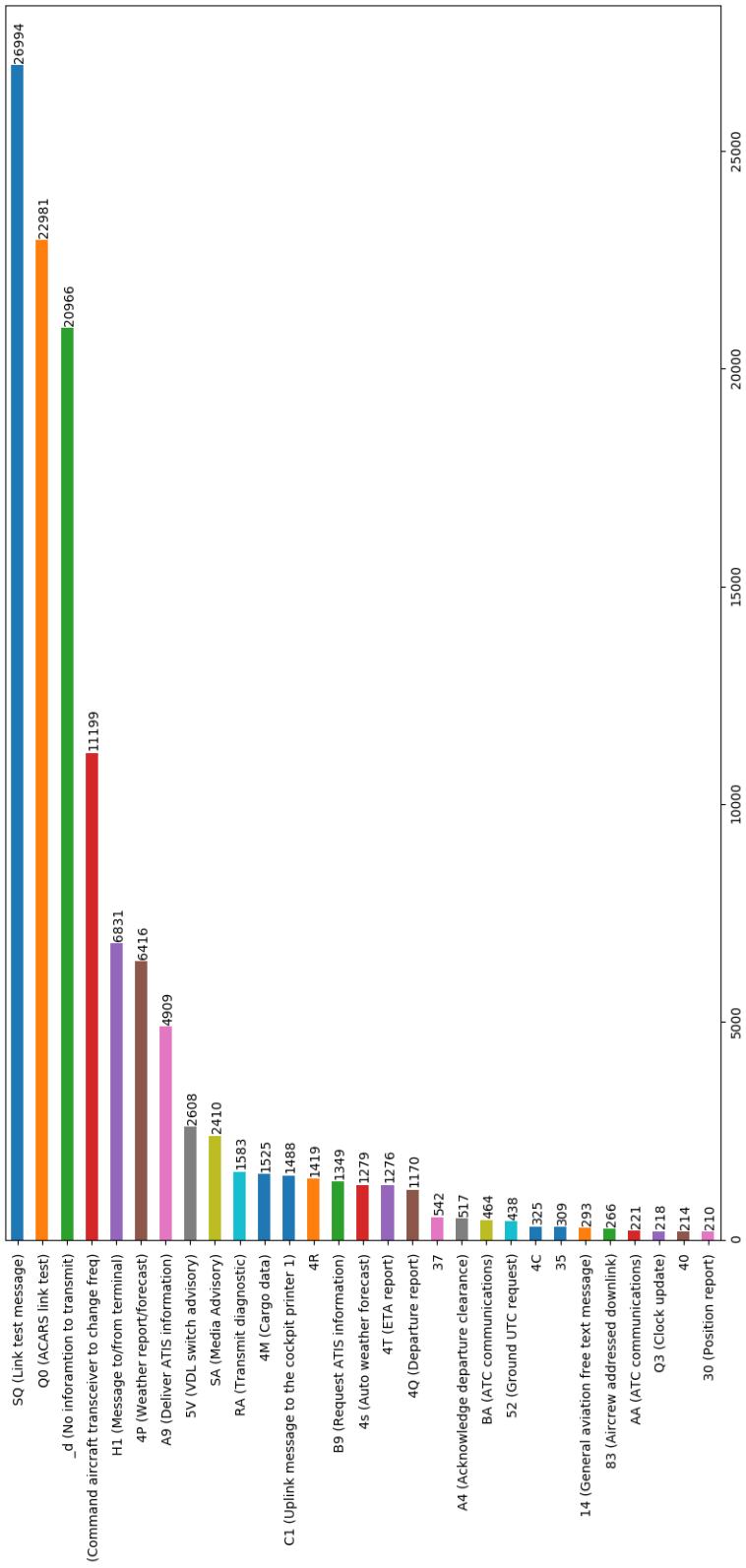


Figure 6.7 Label des messages ACARS reçus

Ces modifications présentent l'inconvénient majeur de nécessiter des ajustements importants dans les solutions déjà mises en place par AMS. En effet, le standard ARINC 823 ne permet pas des communications hors session sécurisées. Il est donc impossible de signer des paquets en dehors de ceux réservés pour le handshake.

La rédaction et l'adoption complète d'un nouveau standard seraient bien évidemment plus longues à mettre en place à grande échelle qu'une simple adoption d'ARINC 823 par tous les appareils commerciaux, car le processus de standardisation est long et coûteux. Nous avons en outre déjà montré que l'adoption immédiate des mesures de sécurité détaillées dans les standards déjà disponibles n'est pas prohibitive du point de vue de l'utilisation de la bande passante ni en termes de sécurité.

6.4 Discussion de l'impact des mesures cryptographiques

Nous l'avons vu, la situation actuelle de la sécurité des communications Datalink est assez critique pour exiger l'adoption rapide de méthodes de protection de l'authentification des paquets échangés.

Dans le cas de l'aéroport de Montréal Trudeau, de nombreuses années sont disponibles avant de faire face à un réel risque de congestion. Les grands aéroports disposent d'environ 20 ans de marge, ce qui est comme nous l'avons vu toujours compatible avec l'utilisation généralisée d'AMS.

L'adoption généralisée d'AMS est utile si elle permet de protéger les communications par liaison de données jusqu'à l'adoption d'ATN qui est développé en intégrant déjà des solutions cryptographiques. Il est difficile de trouver une date exacte pour le déploiement effectif des nouveaux réseaux de communication aéronautique. Un horizon crédible semble être 2025 (Boeing, 2016). Dès lors qu'elles seront disponibles, plusieurs années supplémentaires seront nécessaires à l'adoption par les compagnies des nouvelles technologies Datalink. Ces informations sont résumées sur la figure 6.8

D'après nos prévisions, le déploiement d'ATN sera fait avant qu'un sérieux risque de congestion sur les réseaux ACARS apparaisse, même avec l'utilisation d'AMS . Il est donc aujourd'hui possible (et souhaitable) de transposer rapidement au monde civil les mesures utilisées par les aéronefs militaires sans crainte concernant les capacités des réseaux déjà déployés. Lorsque le risque de congestion sera devenu important, nous pensons que la transition vers ATN aura grandement permis de réduire la charge demandée aux réseaux Datalink historiques comme ACARS et VDL, ce qui réduira d'autant les risques de congestion. L'utilisation d'AMS permettra d'ici la mise en place des réseaux de nouvelle génération de protéger les

communications classiques utilisées par les appareils des différentes attaques que nous avons pu décrire.

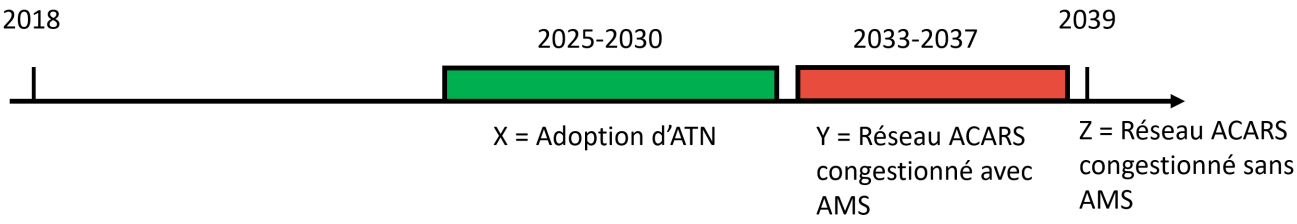


Figure 6.8 Prévision l'évolution des réseaux Datalink (Boeing, 2016).

CHAPITRE 7 CONCLUSION

La situation actuelle de la sécurisation des liaisons de données est complexe. D'une part, de nombreuses solutions existent afin de permettre des communications par liaison de données sécurisées. Les constructeurs d'équipements avioniques ont déjà développé et mis à disposition des compagnies aériennes des équipements compatibles avec AMS permettant la mise en place d'une cryptographie efficace sur ACARS. Nous l'avons également vu, des solutions équivalentes sont en cours d'étude pour FANS1/A et les protocoles utilisant les réseaux VDL tel que CPDLC. Ce sont ces méthodes cryptographiques qui sont utilisées par les appareils militaires et qui leur garantissent dans l'état actuel de nos connaissances une certaine immunité vis-à-vis d'attaque informatique sur leur liaison de données.

A contrario, les compagnies aériennes ne semblent pas encore investir dans de telles solutions. Néanmoins, la récente démocratisation des outils de communications par radio a considérablement facilité l'accès à des moyens de mettre en péril les opérations aériennes. Il est maintenant facile d'interagir avec les liaisons de données. En l'état, les systèmes de communication par liaison de données sont vulnérables, et peuvent servir de support à des attaques dont l'impact est en puissance très élevé.

7.1 Synthèse des travaux

Nos recherches avaient pour objectif de résoudre différents problèmes liés aux questions de recherches suivantes :

Q.1. Quelles sont les failles des communications de liaison de données aéronautiques ?

Il existe de nombreux protocoles de communication par liaison de données. La plupart ont été développés et mis en place alors que les considérations de cybersécurité n'étaient pas une priorité. Ils ne présentent donc aucun mécanisme de protection de leur intégrité, leur authenticité ou leur confidentialité au-delà de ce qu'offrent les procédures nécessaires de leur utilisation.

L'OACI et la communauté scientifique sont au fait de ces failles de sécurités et tentent de promouvoir des mesures de correction. Une version sécurisée d'ACARS, le plus vieux protocole Datalink, a été développée suite aux besoins de l'US Air Force. Un standard propriétaire appelé AMS existe, mais n'est à notre connaissance pas utilisé par les compagnies civiles. De nouveaux réseaux de communications par liaison de donnée et les protocoles associés, regroupés sous le nom d'ATN devraient être mis en place à l'horizon 2025. Si ces derniers

sont développés en intégrant des solutions de sécurité modernes, aucune technique cryptographique efficace ne protège les échanges Datalink jusqu'à l'adoption définitive d'ATN.

Q.2. Jusqu'à quel point une attaque active sur ACARS et/ou FANS 1/A peut-elle influencer le bon déroulement d'un vol commercial ?

Loin de la situation catastrophique décrite par certains chercheurs, il est indéniable qu'il est possible d'exploiter les communications Datalink à des fins malveillantes. Il est possible d'envoyer de fausses informations de contrôle ou d'opérations à un appareil via CPDLC et ACARS. S'il est probablement difficile de déclencher une collision ou d'engendrer la perte d'un appareil, il est définitivement possible de perturber le fonctionnement normal d'un vol commercial.

Nous avons également présenté un scénario d'attaque crédible sur ACARS. Par la modification des données reçues par un appareil lors de la préparation au décollage, il est possible de faire parvenir au pilote d'un appareil de fausses vitesses de décollage. Si l'équipage venait à ne pas mener des vérifications rigoureuses, ce type d'attaque pourrait conduire à un accident de type *tailstrike*, c'est-à-dire une collision de la queue de l'appareil avec la piste lors de la rotation. Nous pensons également qu'il est possible d'envoyer de fausses informations de contrôle à un appareil via CPDLC, ce qui pourrait mener à des déviations de la trajectoire prévue par les contrôleurs pour un appareil. La crédibilité de ces scénarios a été confirmée suite à des échanges informels avec des pilotes de ligne. Cette situation seule présente déjà un problème qu'il est nécessaire d'adresser.

Q.3. Quelle est la difficulté de mener une attaque active sur les communications aériennes par liaison de données ? Quels sont les requis techniques minimums afin d'intercepter et d'émettre des messages de contrôle aérien ?

Nous avons démontré que les prérequis techniques et intellectuels afin de mener une attaque sur les communications par liaison de données sont très faibles. Nous avons développé un signal ACARS complet grâce à un simple USRP et des informations disponibles en ligne. Aucun accès privilégié à une source documentaire n'a été nécessaire afin de développer complètement une preuve de concept. Pour un coût d'environ 1000 CAD et moyennant le travail d'une personne aux connaissances techniques de niveau ingénieur, il est possible de créer de faux signaux ACARS.

Nous pensons donc que tout acteur de menace suffisamment déterminé possède les capacités de mener à bien une attaque sur Datalink. Nous n'avons pas pu vérifier l'efficacité de notre preuve de concept sur un appareil réel pour des raisons légales et logistiques. Néanmoins,

les vérifications que nous avons faites de nos signaux sur des logiciels libres de droits nous permettent d'être confiants quant à son succès sur de véritables systèmes avioniques COTS.

Q.4. Est ce que l'utilisation étendue d'AMS est viable comme moyen de protection des échanges Datalink tant sur le plan technique qu'opérationnel ?

Des standards propriétaires tel que AMS existent déjà pour permettre la mise en place de session de communications ACARS confidentielles entre les appareils militaires et les centres de contrôle. Si ces méthodes ont été pensées et développées pour une utilisation militaire, elles sont également applicables par des appareils commerciaux. Le fait qu'AMS soit soumis à un brevet depuis sa rédaction en 2007 est un frein à sa démocratisation.

Dans une certaine mesure, AMS est adapté à une utilisation dans le cadre des communications aéronautiques civiles. La combinaison des techniques de cryptographie symétrique et asymétrique permet la mise en place de sessions de communications ACARS confidentielles tout en demandant minimum de vérifications aux composantes avioniques embarquées. Cela facilite la rétrocompatibilité avec l'avionique qui ne peut être mise à jour. L'utilisation de réelle de la bande passante n'est pas connue, mais a été évaluée dans la suite de ce mémoire.

La structure exacte d'une PKI nécessaire à l'utilisation des techniques de cryptographie asymétriques n'est pas définie, et sa mise en place prendrait probablement plusieurs années et un effort important de l'OACI et des différents acteurs impliqués. Néanmoins, il s'agit d'une problématique connue et plusieurs pistes comme GateLink existent, bien qu'aucune n'ait encore été déployée à grande échelle.

Si de nombreux travaux proposent des solutions similaires à AMS, aucun standard ne semble être sur le point de voir le jour concernant les protocoles plus récents comme CPDLC. La stratégie actuelle est d'attendre le déploiement complet d'ATN au cours de la prochaine décennie puis d'adapter les nouveaux mécanismes de protection aux futures versions de *FANS1/A over ATN*.

Q.5. Quel serait l'impact sur les réseaux actuels du recours à des solutions cryptographiques du type d'AMS ?

L'utilisation de la cryptographie nécessite l'ajout de nouvelles informations dans les paquets échangés. Nous pensons qu'elle est vitale, mais causera une augmentation de la quantité du trafic sur les réseaux ACARS et VDL. Nous avons collecté des messages pendant 28 jours dans la zone de Montréal afin d'évaluer les conséquences de l'adoption massive de la cryptographie. Ces données nous ont servi de base à une étude statistique sur l'impact des mesures cryptographiques sur le réseau.

L'ajout d'un HMAC, même de 128 bits, à la fin des paquets pour garantir leur intégrité est négligeable face à la quantité de paquets déjà envoyés sur le réseau. Seuls les handshakes nécessaires pour la création d'un secret partagé augmentent sensiblement le nombre de communications.

La perte associée à l'utilisation de versions sécurisées des communications ACARS comme AMS représente 2 à 6 ans de croissance normale du trafic et n'est donc pas prohibitive concernant l'adoption des méthodes de protections militaires par le monde civil. Nos estimations nous permettent de penser que le déploiement des réseaux Datalink de nouvelle génération comme ATN sera fait antérieurement à l'apparition d'un sérieux risque de congestion sur les réseaux ACARS et VDL, même avec l'utilisation d'AMS. Nous pensons donc qu'il est tout à fait adapté d'avoir recourt à AMS pour protéger les communications actuelles.

Si d'aventure le risque de congestion devenait trop élevé, nous pensons qu'il est possible de développer de nouveaux standards plus adaptés à l'aéronautique civile. Il n'est en effet pas nécessaire de garantir la confidentialité des communications par liaison de données. Cela ne pose pas réellement un risque de sécurité et certains pays ne souhaitent pas que les avions qui survolent leurs espaces aériens aient des communications privées. Des signatures digitales basées sur la cryptographie asymétrique permettraient d'assurer un niveau de sécurité satisfaisant vis-à-vis des attaques que nous avons détaillées sur les vitesses au décollage et l'envoi de messages de contrôle non authentifiés, tout en réduisant l'impact des mesures cryptographiques sur le réseau.

7.2 Limitations de la solution proposée

Nos travaux présentent plusieurs limitations qu'il convient de relever. Nos tests sont pour la plupart basés sur les paquets ACARS que nous avons écoutés à proximité de l'aéroport YUL de Montréal. Le trafic aérien de cette zone n'est peut-être pas représentatif du reste du paysage aéronautique. En outre, les problématiques de gestion des fréquences et de la bande passante sont probablement plus complexes dans les grands aéroports, car les fréquences VHF, HF et Satcom y sont plus sollicitées. Nous avons pu obtenir un ordre de grandeur de l'utilisation déjà faite des bandes de fréquences dans ces zones en comparant le trafic aérien, mais une analyse plus fine serait probablement nécessaire.

Concernant notre preuve de concept d'attaque, si nous avons réussi à développer un prototype pouvant aisément envoyer de faux messages ACARS, son efficacité n'a pas pu être démontrée sur un système réel. Afin de prouver définitivement le danger qui pèse actuellement sur les appareils commerciaux, il est important de mener de telles validations sur des composantes

avioniques COTS. Ceci serait possible via l'achat des composantes nécessaires ou l'envoi de paquets vers des appareils commerciaux. Néanmoins, comme nous l'avons déjà expliqué, nous ne présentons que très peu de réserves quand à l'éventuel succès de notre attaque en dehors d'un environnement simulé car les décodeurs employés ont déjà été validés sur des paquets réels.

En outre, nous nous sommes concentrés sur la technologie ACARS sur son réseau classique sur ondes VHF (non VDL). Bien qu'elle soit encore fortement utilisée, elle est la plus ancienne de toutes les liaisons de données et possède une utilisation limitée aux communications AOC. Des travaux similaires sont nécessaires sur les protocoles plus récents comme CPDLC et ACARS sur les réseaux VDL, et qui seront adaptés pour ATN dans les années qui viennent. Néanmoins, nous ne nous attendons pas à voir apparaître de problème de congestion sur ces technologies qui sont plus performantes et seront également portée sur ATN une fois sa mise en place effective.

Enfin, nous défendons l'adoption d'AMS pour la sécurisation des communications Datalink. Néanmoins, cette solution présente plusieurs inconvénients. Il s'agit d'un standard propriétaire, ce qui est un frein non négligeable à son développement par les fabricants d'avionique. Honeywell possède un brevet sur la méthode d'implémentation d'AMS qui sera valable jusqu'en 2027. En outre, la mise en place d'une PKI adaptée est délicate. Si certaines structures sont déjà en place (Gate Link, PKI de l'OACI pour la gestion des passeports électroniques etc), aucune solution n'est réellement opérationnelle aujourd'hui et elles doivent toute faire leur preuve pour une éventuelle utilisation à grande échelle. Si la mise en place d'une telle PKI demande des efforts considérables, nous ne pensons pas qu'ils soient prohibitifs. Les nombreux efforts récents dans le domaine présentés par l'OACI et les différentes acteurs industriels nous laissent penser que la problématique du déploiement d'une PKI adaptée aux contraintes des communications aéronautiques est connue et sur le point d'être résolue dans les années qui viennent.

Enfin, il s'agit d'une version d'ACARS développée avec comme objectif principal de garantir la confidentialité des paquets. Certains pays membres de l'OACI ne souhaitent peut être pas que les appareils empruntant les zones aériennes sous leur contrôle aient recourt à de tels mécanismes de protection des données. Enfin, la structure de la PKI exacte qui serait nécessaire à une utilisation généralisée dans l'aviation civile d'AMS n'est toujours pas définie. Sa mise en place et sa gestion représentent des problématiques complexes qu'il conviendrait d'adresser plus en détail.

7.3 Améliorations futures

Si nos travaux ont permis d'éclaircir et de détailler les menaces qui pèsent sur les communications par liaison de données, nous pensons que certaines pistes d'amélioration sont envisageables.

Dans un premier temps, il pourrait être pertinent de détailler précisément tous les scénarios d'attaques possibles basés sur l'exploitation du manque de contrôle de l'authenticité et de l'intégrité des protocoles Datalink. Cela permettrait de cerner encore mieux le risque actuel qui pèse sur les avions commerciaux en décrivant la totalité des risques présents.

En outre, le standard AMS que nous avons longuement étudié, bien qu'il nous semble adapté, est perfectible. Il engendre une dégradation supportable, mais notoire, de la quantité de trafic sur les réseaux. Nous ne pensons pas que la confidentialité des communications soit nécessaire ni même souhaitable (afin de rester en adéquation avec les souhaits de tous les pays membres de l'OACI). En considérant cela, des travaux supplémentaires sont nécessaires afin d'approfondir les pistes de travail que nous avons proposé quant à la rédaction de nouveaux standards de sécurité, basés sur la cryptographie asymétrique et non propriétaires. Ces mêmes travaux devraient prendre en considération les protocoles plus récents qui utilisent les réseaux VDL comme CPDLC. Ceci empêcherait de maintenir la politique d'attente actuelle, car l'adoption d'ATN est encore lointaine.

RÉFÉRENCES

R. Abeyratne, “Cyber terrorism and aviation—national and international responses”, *Journal of Transportation Security*, vol. 4, no. 4, pp. 337–349, 2011.

ACI, “ACI World releases preliminary 2017 world airport traffic rankings Passenger traffic : Indian and Chinese airports major contributors to growth Air cargo : Volumes surge at major hubs as trade wars threaten”, 2017. En ligne : `http://www.aci.aero/News/Releases/Most-Recent/2018/04/09/ACI-World-releases-preliminary-2017-world-airport-traffic-rankings--Passenger-traffic-Indian-and-Chinese-airports-major-contributors-to-growth---Air-cargo-Volumes-surge-at-major-hubs-as-trade-wars-threaten-`

A.F.MacDonald, *From the Ground Up.* Aviation Publishers Co.Ltd, 2011.

Airbus Training and Flight Operations Support and Services, “A318/A319/A320/A321 flight performance training manual”, 2005.

Airsafe, “Average fleet age for selected airlines”, Jan. 2016. En ligne : `http://www.airsafe.com`

L. K. Anderson, *ACARS a Users Guide.* Las Atalayas Publishing, 2010.

ANSI, X9, “62 : Public key cryptography for the financial services industry : The elliptic curve digital signature algorithm (ECDSA)”, *Am. Nat’l Standards Inst*, 1999.

J. Arasly, “Terrorism and civil aviation security : Problems and trends”, *Connections : The Quarterly Journal*, vol. 4, no. 1, pp. 75–89, 2005.

ARINC, “ARINC 618-8 Air/Ground Character-Oriented Protocol Specification”, Standard, Août 2016.

——, “ARINC 823 Part 1 ACARS Message Security (AMS)”, ARINC, Standard, Déc. 2007.

——, “ARINC 823 Part 2 AMS Key management”, ARINC, Standard, Mars 2008.

ARINC Working Group M, “ARINC’s response to VDL mode 2 technical manual deficiencies and additional changes proposal”, 2000.

"A4A SPEC 42 : Aviation Industry Standards for Digital Information Security", ATA, Standard, Jan. 2017.

ATNP Working Groups, "Global operational data link document", 1999. En ligne : www.mccallumwhyman.com/downloads/Guidance%20Material/parti.pdf

ATSB, "ATSB transport safety report aviation occurrence investigation AO-2009-012 final", Déc. 2009. En ligne : www.atsb.gov.au/media/3531728/ao2009012_full%20report.pdf

BEA, "Accident on 24 march 2015 at Prads-Haute-Bléone (alpes-de-haute-provence, france) to the airbus a320-211 registered D-AIPX operated by germanwings - final report", Mars 2016. En ligne : www.bea.aero/uploads/tx_elydbrapports/BEA2015-0125.en-LR.pdf

M. Bellare, R. Canetti, et H. Krawczyk, "Keying hash functions for message authentication", dans *Crypto*, vol. 96. Springer, 1996, pp. 1–15.

Boeing, "ATS data link deployment aircraft manufacturer's perspective", 2016. En ligne : www.icao.int/APAC/Meetings/2016%20FITAsia5/P17%20-%20ATS%20data%20link%20deployment%20%20Aircraft%20Manufacturers%20perspective.pdf

C. Bresteau, S. Guigui, P. Berthier, et J. M. Fernandez, "On the security of aeronautical Datalink communications : Problems and solutions", dans *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, April 2018.

Eurocontrol, "Network handling record numbers of flights | Eurocontrol". En ligne : http://www.eurocontrol.int/news/network-handling-record-numbers-flights

FAA, "Guidelines for design approval AC No : 20-140b", Sep. 2012. En ligne : www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-140B.pdf

Gouvernement du Canada, "Archives météo canadiennes", Jan. 2018. En ligne : http://climat.meteo.gc.ca/climate_data/daily_data_f.html?StationID=48374&timeframe=2&StartYear=1840&EndYear=2018&Day=1&Year=2017&Month=12

M. Gregorova, "Eurocontrol long-term forecast : Flight movements 2010–2030", *CND/STATFOR Doc415, Eurocontrol, Brussels*, 2010.

A. Helfrick, *Principles of Avionics Seventh Edition*. Avionics Communications INC, 2012.

B. Hilburn et J. Corgan, "Gnuradio", 2017. En ligne : www.gnuradio.org/

Honeywell, “ACARS message security (AMS) as a vehicle for validation of ICAO doc. 9880 part iv-b security requirements”, Juin 2009. En ligne : www.icao.int/safety/acp/ACPWGF/ACP-WG-M-14/ACP-WGM-IP07%20-%20AMS%20for%209880%20Security%20Validation_20090604%20(HON-Olive).pdf

ICAO, “Regulations for the ICAO public key directory”, march 2011.

——, “9705-AN/956 : Manual of technical provisions for the aeronautical telecommunication network ATN”, Rapp. tech., 2002.

——, “9880-AN/466 : Manual on detailed technical specifications for the aeronautical telecommunication network ATN using ISO”, Rapp. tech., 2010.

——, “Global operational data link document”, Avr. 2013. En ligne : www.icao.int/APAC/Documents/edocs/GOLD_2Edition.pdf

INCITS, ANSI, “ISO/IEC 13239 : 2002”, *Information technology–Telecommunications and information exchange between systems–High-level Data Link Control (HDLC) procedures*.

L. Kleinrock et F. Tobagi, “Packet switching in radio channels : Part I–carrier sense multiple-access modes and their throughput-delay characteristics”, *IEEE transactions on Communications*, vol. 23, no. 12, pp. 1400–1416, 1975.

T. Kraft, “FANS1/A and data link operations benefits, challenges and opportunities”, dans *USAF CNS/ATM Conference 2009*. FAA, 2009.

A. Lam, J. Fernandez, et R. Frank, “Cyberterrorists bringing down airplanes : Will it happen soon ?” dans *International Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited, 2017, p. 210.

T. Lemiech, “Dumpvdl2”, 2017. En ligne : github.com/szpajder/dumpvdl2

S. Lundström, “Technical details of VDL mode 2”, Mars 2016. En ligne : www.commsys.isy.liu.se/TSKS03/reports/VDL-M2.pdf

M. S. B. Mahmoud, N. Larrieu, et A. Pirovano, “An aeronautical data link security overview”, dans *Digital Avionics Systems Conference, 2009. DASC’09. IEEE/AIAA 28th*. IEEE, 2009, pp. 4–A.

M. S. B. Mahmoud, N. Larrieu, A. Pirovano, et A. Varet, “An adaptive security architecture for future aircraft communications”, dans *Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th.* IEEE, 2010, pp. 3–E.

M. S. B. Mahmoud, N. Larrieu, et A. Pirovano, “Aeronautical communication transition from analog to digital data : A network security survey”, *Computer Science Review*, vol. 11, pp. 1–29, 2014.

A. Mattos, “SITA AIRCOM service - VHF and satellite”, Jan. 2009. En ligne : `sonicboom.aero/wp-content/uploads/sites/11/2011/01/SITA_AIRCOM_Service_{ACARS}_Network.pdf`

V. S. Miller, *Use of Elliptic Curves in Cryptography.* Berlin, Heidelberg : Springer Berlin Heidelberg, 1986, pp. 417–426. En ligne : `https://doi.org/10.1007/3-540-39799-X_31`

Ministère de la Justice, “Règlement de l’aviation canadien DORS/96-433”, Sep. 1996. En ligne : `laws-lois.justice.gc.ca/fra/reglements/DORS-96-433/TexteComplet.html`

M. S. Nolan, *Fundamentals of Air Traffic Control.* Delmar Cengage Learning, 2011.

M. Olive, “Efficient datalink security in a bandwidth-limited mobile environment-an overview of the aeronautical telecommunications network ATN security concept”, dans *Digital Avionics Systems, 2001. DASC. 20th Conference*, vol. 2. IEEE, 2001, pp. 9E2–1.

E. Perez, “FBI : Hacker claimed to have taken over flight’s engine controls”, *CNN*, 2015.

P. Rajeswari et K. Thilagavathi, “An efficient authentication protocol based on elliptic curve cryptography for mobile networks”, *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 2, pp. 176–85, 2009.

C. Risley, J. McMath, et B. Payne, “Experimental encryption of aircraft communications addressing and reporting system (ACARS) aeronautical operational control (AOC) messages”, dans *Digital Avionics Systems, 2001. DASC. 20th Conference*, vol. 2. IEEE, 2001, pp. 7D4–1.

A. Roy, “Secure aircraft communications addressing and reporting system (ACARS)”, dans *Digital Avionics Systems, 2001. DASC. 20th Conference*, vol. 2. IEEE, 2001, pp. 7A2–1.

K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, et C. Royalty, “Future e-enabled aircraft communications and security : The next 20 years and beyond”, *Proceedings of the IEEE*, vol. 99, no. 11, pp. 2040–2055, 2011.

D. Selleck, “Iridium fault prompts ban by oceanic ATC”, Oct. 2017. En ligne : flightservicebureau.org/iridium-fault/

SITA, “SITA data link”, Avr. 2016. En ligne : www.icao.int/NACC/Documents/Meetings/2016/ATS/DATALINKP14.pdf

M. Smith, M. Strohmeier, V. Lenders, et I. Martinovic, “On the security and privacy of ACARS”, dans *Integrated Communications Navigation and Surveillance (ICNS), 2016*. IEEE, 2016, pp. 1–27.

N. Smith, J. Brown, P. Polson, et J. Moses, “An assessment of flight crew experiences with FANS-1 controller-pilot data link communication in the South Pacific”, dans *4th USA/Europe Air Traffic Management R&D Seminar*, 2001.

W. Stallings et L. Brown, *Computer Security : Principles and Practice (3rd Edition)*. Pearson, 2014.

P. E. Storck, “Benefits of commercial data link security”, dans *Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, 2013, pp. 1–6.

M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, et I. Martinovic, “On perception and reality in wireless air traffic communication security”, *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1338–1357, 2017.

B. Sveen, “Passenger plane forced to abort landing after receiving hoax radio call at Melbourne airport”, November 2016, [Online ; posted 7-November-2016]. En ligne : www.abc.net.au/news/2016-11-07/afp-investigating-hoax-calls-made-to-passenger-plane/7995502

H. Teso, “Aircraft hacking practical aero series”, 2013. En ligne : conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf

Tomsk State University of Systems Control and Radioelectronics, “AcarsDeco - xDeco.org”, 2016. En ligne : xdeco.org/?page_id=42

Transport Canada, *Manuel d’information Aeronautique*, 2016.

C. Trautvetter, “Honeywell debunks reports of bogus CPDLC messages”, Jan. 2017. En ligne : www.ainonline.com/aviation-news/business-aviation/2017-01-16/honeywell-debunks-reports-bogus-cpdlc-messages

UASC, “Understanding data comm systems with FANS1/A+,CPDLC DCL and ATN B1”, Jan. 2017. En ligne : www.uasc.com/docs/default-source/documents/whitepapers/uasc_fans_whitepaper.pdf?sfvrsn=d81d985c_4

M. Yue et X. Wu, “The approach of ACARS data encryption and authentication”, dans *Computational Intelligence and Security (CIS), 2010 International Conference on.* IEEE, 2010, pp. 556–560.

R. E. Ziemer et W. H. Tranter, *Principles of Communications.* John Wiley Sons INC, 2009.